

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

PCT

世界知的所有権機関
国際事務局

特許協力条約に基づいて公開された国際出願



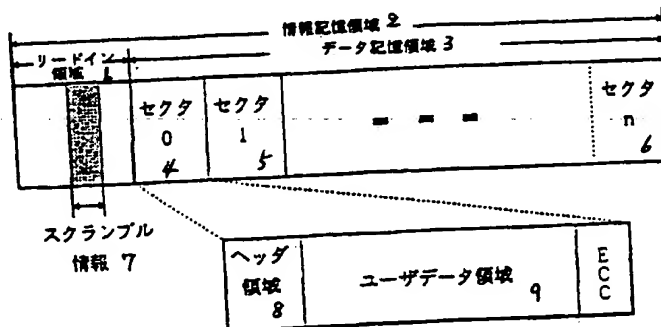
(51) 国際特許分類6 G11B 19/00	A1	(11) 国際公開番号 WO97/14147
		(43) 国際公開日 1997年4月17日(17.04.97)
(21) 国際出願番号 PCT/JP96/02901	1996年10月4日(04.10.96)	(74) 代理人 松崎なつめ(MATSUZAKI, Natsume)[JP/JP] 〒562 大阪府箕面市粟生間谷西一丁目6-7-803 Osaka, (JP)
(22) 国際出願日		(74) 代理人 弁理士 山本秀策(YAMAMOTO, Shusaku) 〒540 大阪府大阪市中央区城見一丁目2番27号 クリスタルタワー15階 Osaka, (JP)
(30) 優先権データ 特願平7/261266	1995年10月9日(09.10.95)	(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)(JP/JP) 〒571 大阪府門真市大字門真1006番地 Osaka, (JP)	JP	添付公開書類 国際調査報告書 請求の範囲の補正の期限前であり、補正書受領の際には再公開される。
(72) 発明者：および (75) 発明者／出願人 (米国についてのみ) 植田 宏(UEDA, Hiroshi)[JP/JP] 〒573 大阪府枚方市御殿山南町4-3426 Osaka, (JP) 福島能久(FUKUSHIMA, Yoshihisa)[JP/JP] 〒536 大阪府大阪市城東区関目六丁目14番C-508 Osaka, (JP) 伊藤基志(ITO, Motoshi)[JP/JP] 〒536 大阪府大阪市城東区古市三丁目17番25-302号 Osaka, (JP) 館林 誠(TATEBAYASHI, Makoto)[JP/JP] 〒665 兵庫県宝塚市売布一丁目16-21 Hyogo, (JP)		

(54) Title: INFORMATION RECORDING MEDIUM, INFORMATION REPRODUCTION APPARATUS AND INFORMATION REPRODUCTION METHOD

(54) 発明の名称 情報記録媒体、情報再生装置および情報再生方法

(57) Abstract

An information recording medium including a lead-in region and a data recording region, wherein key information is recorded in the lead-in region and scrambled data are recorded in the data recording region. The scrambled data are descrambled on the basis of the key information.



- 1 ... lead-in region
- 2 ... information storage region
- 3 ... data storage region
- 4 ... sector 0
- 5 ... sector 1
- 6 ... sector n
- 7 ... scrambled information
- 8 ... header region
- 9 ... user data region

(57) 要約

情報記録媒体は、リードイン領域とデータ記録領域とを有している。リードイン領域には、鍵情報が記録される。データ記録領域には、スクランブルされたデータが記録される。スクランブルされたデータは、鍵情報に基づいてデスクランブルされる。

情報としての用途のみ

PCTに基づいて公開される国際出願をパンフレット第一頁にPCT加盟国を同定するために使用されるコード

AL	アルバニア	EE	エストニア	LR	リベリア	RU	ロシア連邦
AM	アルメニア	EF	エストニア	LS	レソト	DE	ドイツ
AT	オーストリア	FR	フランス	LT	リトアニア	SE	スウェーデン
AZ	アゼルバイジャン	GB	イギリス	LU	ルクセンブルグ	SI	スロベニア
BG	ブルガリア	GE	グルジア	LV	ラトヴィア	SK	スロバキア
BE	ベルギー	GH	ガーナ	MC	モナコ	KN	セント・キッツ
BF	ブルキナファソ	GN	ギニア	MD	モルドバ	NZ	ニュージーランド
BJ	ベナン	GR	ギリシャ	MG	マダガスカル	SD	スーダン
BR	ブラジル	HU	ハンガリー	MK	マケドニア	SG	シンガポール
BY	ベラルーシ	IE	アイルランド	VL	ヴァチカン	SI	スロベニア
CA	カナダ	IS	アイスランド	ML	マリ	TM	トルクメニスタン
CC	中東	IT	イタリア	MN	モンゴル	TR	トルコ
CF	中央アフリカ共和国	JP	日本	MR	モーリタニア	TT	トリニダード・トバゴ
CG	コンゴ	KE	ケニア	MW	マラウイ	UA	ウクライナ
CH	スイス	KR	韓国	MX	メキシコ	UG	ウガンダ
CI	コート・ジボアール	KG	キルギス	NE	ニジェール	US	米国
CM	カメルーン	KP	朝鮮民主主義人民共和国	NL	オランダ	UZ	ウズベキスタン
CN	中国	KZ	カザフスタン	NO	ノルウェー	VN	ベトナム
CZ	チェコ共和国	LI	リヒテンシュタイン	NZ	ニュージーランド	YU	ユーゴスラビア
DE	ドイツ	LK	スリランカ	PT	ポルトガル		
DK	デンマーク			RO	ルーマニア		

明 細 書

情報記録媒体、情報再生装置および情報再生方法

5 技術分野

本発明は、プログラムデータ、音声情報、映像情報を含む情報信号を記録する情報記録媒体と、情報記録媒体に記録された情報を再生する情報再生装置および情報再生方法とに関する。

10 背景技術

従来、プログラムデータや音声情報、映像情報の情報記録媒体としては、フロッピーディスクやCD-ROM (Compact Disk - Read Only Memory) などが知られている。特にCD-ROMは、600MB以上の大容量を有することや制作費用が安価になったこと等の理由で、各種ソフトウェアの頒布にさかんに用いられている。

一方、近年のパーソナルコンピュータの高速化によって、パーソナルコンピュータ上で映像および音声データ（以下、AVデータと称す）を出力する需要が急速に高まっている。例えばMPEG1 (Moving Picture Experts Group) と呼ばれる映像圧縮方式を用いてデータ圧縮を施したデジタルデータファイルを、CD-ROMなどに記録して頒布するようなアプリケーションが増加している。しかしながらMPEG1方式は一般に、大容量となる映像データを高い圧縮率を用いて圧縮するために、映像の劣化も著しい。従って、映画等の高品質な映像を要求される用途には不適當であった。

そこで近年、5GB近い大容量を有する光ディスクにMPEG2方式と呼ばれる、より高度な映像圧縮方式を用いて、高品質な映像データを記録する開発が行われている。DVD (Digital Video Disk) と呼ばれるその光ディスクは、大容

量性を生かして、2時間以上もの高品質なデジタルAVデータを記録することが可能であり、次世代のAVデータ記録媒体として大いに期待されている。またその一方でDVDは、パーソナルコンピュータと接続されてDVDを再生するDVDドライブによって、高品質なAVデータをパーソナルコンピュータ上で再生
5 することが可能となるとともに、計算機ソフトウェアの頒布媒体としてもCD-ROMに替わる情報記録媒体として期待されている。

しかしながら、パーソナルコンピュータの周辺装置としてのDVDドライブが市場に出回れば、DVDに記録されたデジタルデータがパーソナルコンピュータに出力され、容易にハードディスクやMO (Magneto Optical Disk) 等の書き
10 換え型メディアにコピーすることが可能となる。前記のようなデジタルAVデータのコピーが容易に行えれば、DVDに記録されたAVデータがその著作者の許可なく違法にコピーされたり、改竄を施されて頒布されるなどの問題が生じ、著作者の権利を保護することが極めて困難となる。このことは、データの著作者にとって不利益をもたらすばかりでなく、著作者がコピーされることを考慮して
15 価格設定を行うことやデータの改竄をおそれてディスクの製造を行わない等の措置がとられた場合においては、ユーザへの不利益も生ずる可能性がある。前記の課題を以下では、第1の課題と称する。

一方、AVデータの記録された情報記録媒体の用途としては、様々な用途が考えられる。これらの用途の中には、情報記録媒体があらゆる再生装置で再生可能
20 となることが逆に問題となる用途も存在し、その様な用途では再生可能な再生装置と再生不可能な再生装置とに分割できることが好ましい。例えば、一般にカラオケディスクと呼ばれるような、再生される音楽に合わせてその歌詞を含んだ映像データが記録されるようなディスクには、一般家庭で個人的に使用されるディスク（以下、民生用ディスクと称す）と、利用客が一定の料金を支払ってカラオケを楽しむような施設において使用されるディスク（以下、業務用ディスクと称す）とが存在する。業務用ディスクが限られた使用者に大量に納入することを前
25

提に製造されるために、低価格で供給されるのに対し、民生用ディスクは単品販売のために比較的高価格で販売されている。’

しかしながら、業務用ディスクと民生用ディスクとが全く同一フォーマットであった場合には、業務用ディスクが民生用として一般市場で安価に販売される可能性
5 がある。従って、市場における民生用ディスクの適正な価格での流通を妨げ、ディスク製造者および正規に民生用ディスクを購入するユーザの不利益となる。従ってこの様な用途では、民生用ディスクと業務用ディスクで再生可能な再生装置が分離できることが望ましい。また別の例としては、倫理的な問題のある内容を記録したディスクを再生する場合がある。倫理的な問題があるか否かを判定する
10 基準は各国ごとに異なる。従ってある国では再生されるべきディスクが、他の国で再生されるのが望ましくない場合が生ずる。従って、倫理上問題があるディスクはその販売が許可される特定の国でのみ再生されるような仕組みが必要である。以上の様に、ディスクの用途に応じて再生可能な再生装置と再生不可能な再生装置とを分割できないという課題があった。この課題を、以下では第2の課題
15 と称する。

上記の2つ課題を解決するための一つの手段として、情報記録ディスクに記録するデータをスクランブル（又は暗号化）して記録する方法がある。すなわち、前記第1の課題に対しては、パーソナルコンピュータにおけるコピー動作時に、ある鍵をもとにスクランブルの施されたデータを返送し、デスクランブルするための鍵を返送しないことによりコピー動作を防止できる（コピー動作は行われる
20 が、そのデスクランブルが行えないために、コピー動作の意味をなさない）。

また、前記第2の課題に対しては、ディスクの内容に応じて異なるスクランブルを施したディスクを作成することで、デスクランブル可能な装置とデスクランブル不可能な装置とを分類できる。このように、記録データのスクランブル（又は暗号化）は前記の2つの問題に有効であるが、データをデスクランブルするための方法又は鍵をどのように指定するかが問題となる。
25

データ領域に暗号化を施す第1の従来例として、特開平7-249264号公報の図3のCD-ROMでは、暗号化されたデータセクタとは異なるセクタのメインデータ領域に暗号鍵を記録する方式が提案されている。本従来例では、記録時に暗号化されたデータとその暗号鍵をCD-ROMに記録し、再生時にはパーソナルコンピュータから再生装置に対して暗号鍵の読み出し命令を行った後に暗号化データを復号することにより、データ再生を実現するというものである。本方法は、暗号鍵の変更が容易に行えるという利点がある。

また、第2の従来例として、特開平7-85574号公報の図3に示されるように再生装置の光ヘッドが走査しないディスクの領域に暗号化キーを記録する方式が提案されている。本従来例では、一般のパーソナルコンピュータから暗号鍵を読み出されることを防止するために、コピー動作において暗号鍵はコピーされず、違法なコピー動作が意味をなさない。

しかしながら、前記第1の従来法の暗号鍵はセクタのメインデータ領域に記録されているため、係るディスクの記録時に用いられた暗号鍵を一般のパーソナルコンピュータから容易に読み出すことができる。従って、暗号鍵と暗号化データをユーザが読み出すことができるために、暗号の解読が行われる危険性が高い。

また第2の従来法では、暗号鍵を再生装置の光ヘッドが走査しない領域に記録するために、暗号鍵を読み出すためにはデータ記録領域からデータを読み出す読み出し手段に加えて暗号鍵読み出し専用の読み出し手段が必要になるという問題が生ずる。

本発明は、情報記録媒体に記録された内容が違法にコピーされることを確実に防止する強固な著作権保護を実現するためのデータ構造を有する情報記録媒体と、特別なデータ読み出し手段を設けることなく前記情報記録媒体からのデータ再生が可能であり、かつ、前記課題1および2を解決するための情報再生装置および情報再生方法を提供することを目的とする。

発明の開示

本発明の情報記録媒体は、リードイン領域とデータ記録領域とを有する情報記録媒体であって、該リードイン領域には、鍵情報が記録され、該データ記録領域には、スクランブルされたデータが記録され、該スクランブルされたデータは、
5 該鍵情報に基づいてデスクランブルされる。

本発明の他の情報記録媒体は、リードイン領域とデータ記録領域とを有する情報記録媒体であって、該リードイン領域には、第1の鍵情報が記録され、該データ記録領域には、第2の鍵情報と、スクランブルされたデータとが記録され、該スクランブルされたデータは、該第1の鍵情報に基づいて該第2の鍵情報を変換
10 することによって得られる情報に基づいてデスクランブルされる。

ある実施形態では、前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記第2の鍵情報は、該セクタヘッダ領域に記録されている。

15 他の実施形態では、前記第2の鍵情報は、前記第1の鍵情報によって暗号化されており、前記情報は、該暗号化された第2の鍵情報を復号化することによって得られる。

他の実施形態では、前記第1の鍵情報は、マスター鍵情報によって暗号化されている。

20 他の実施形態では、前記リードイン領域には、複数の第1の鍵情報が記録されており、該複数の第1の鍵情報は、複数の異なるマスター鍵情報によってそれぞれ暗号化されている。

他の実施形態では、前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録
25 されている。

他の実施形態では、前記データ記録領域は、複数のセクタに分割されており、

該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記スクランブルフラグは、該セクタヘッダ領域に記録されている。

5 他の実施形態では、前記データ記録領域は、複数のファイルを記録する領域と、該複数のファイルを管理する情報を記録するファイル管理領域とを含んでおり、前記スクランブルフラグは、該ファイル管理領域に記録されている。

10 他の実施形態では、前記リードイン領域には、前記スクランブルされたデータを読み出す読み出し装置と該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置との間で相互認証を行うための相互認証鍵情報がさらに記録されている。

他の実施形態では、前記情報は、乱数系列を生成するための初期値であり、前記スクランブルされたデータは、該乱数系列に対して論理演算を行うことによりデスクランブルされる。

15 他の実施形態では、前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記情報記録媒体の用途を識別する情報が該セクタヘッダ領域に記録されている。

20 本発明の情報再生装置は、情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード装置に送信することを認証する認証回路とを備えている。

25 ある実施形態では、前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領域に記録される第2の鍵情報とを含む。

本発明の他の情報再生装置は、情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置から、該スクランブルされたデータを受信する前に、該鍵情報に対応する情報を該読み出し装置から受信することを認証する認証回路と、
5 該読み出し装置から受信した該スクランブルされたデータをデスクランブルするデスクランブル回路とを備えている。

ある実施形態では、前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領域に記録される第2の鍵情報とを含む。

10 他の実施形態では、前記デスクランブル回路は、該第1の鍵情報に基づいて該第2の鍵情報を変換することによって得られる情報に基づいて前記スクランブルされたデータをデスクランブルする。

本発明の他の情報再生装置は、情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、該スクランブルされたデータをデスクランブルする
15 デスクランブル回路を含むデコード部と、該デコード部に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード部に送信することを認証する認証回路とを備えている。

ある実施形態では、前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、
20 該データ記録領域に記録される第2の鍵情報とを含む。

他の実施形態では、前記デスクランブル回路は、該第1の鍵情報に基づいて該第2の鍵情報を変換することによって得られる情報に基づいて前記スクランブルされたデータをデスクランブルする。

25 他の実施形態では、前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録

されており、前記情報再生装置は、該スクランブルフラグに応じて、前記認証回路を起動するか否かを制御する制御回路をさらに備えている。

他の実施形態では、前記認証回路による認証は、所定の関数を用いて行われる。

5 他の実施形態では、前記認証回路による認証は、時間と共に変化する情報を用いて行われる。

 他の実施形態では、前記認証回路は、認証処理が正常に終了した場合にバス鍵情報を生成し、該バス鍵情報を用いて前記第 1 の鍵情報と前記第 2 の鍵情報とを暗号化する。

10 他の実施形態では、前記認証回路は、前記バス鍵情報を用いて前記暗号化された第 1 の鍵情報と前記暗号化された第 2 の鍵情報とを復号化する。

 本発明の情報再生方法は、情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置と、該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置とを用いて、該スクランブルされたデータを再生する情報再生方法であって、該読み出し装置と該デコード装置との間で相互認証処理を行うステップと、該読み出し装置と該デコード装置との間で相互認証処理が正常に終了した場合に、該読み出し装置と該デコード装置とに共通するバス鍵情報を生成するステップと、該バス鍵情報に応じて該鍵情報を暗号化するステップと、該暗号化された鍵情報を該読み出し装置から該デコード装置に送信するステップとを包含する。

15 20

図面の簡単な説明

 図 1 は、本発明に係る情報記録媒体のデータ構造を示す図である。

25 図 2 (a) および (b) は、図 1 に示す情報記録媒体のリードイン領域に記録されるスクランブル情報の構造を示す図である。

 図 3 は、本発明に係る情報記録媒体の他のデータ構造を示す図である。

図 4 は、本発明に係る情報再生装置の構成を示すブロック図である。

図 5 は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図 6 は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図 7 は、本発明に係る情報再生装置の他の構成を示すブロック図である。

5 図 8 は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図 9 (a) ~ (c) はスクランブル処理方法の一例を説明するための図である。

図 10 (a) ~ (f) は、本発明に係る情報記録媒体のデータ構造を示す図である。

10 図 11 (a) ~ (c) は、ボリューム・ファイル管理領域中のディレクトリレコードのデータ構造を示す図である。

図 11 (d) は、スクランブル情報セクタのデータ構造を示す図である。

図 11 (e) は、スクランブルセクタのデータ構造を示す図である。

図 11 (f) は、非スクランブルセクタのデータ構造を示す図である。

図 12 (a) ~ (c) は、スクランブル方式の一例を説明するための図である。

15 図 13 (a) ~ (c) は、ボリューム・ファイル管理領域中のディレクトリレコードのデータ構造を示す図である。

図 13 (d) は、スクランブル情報セクタのデータ構造を示す図である。

図 13 (e) は、スクランブルセクタのデータ構造を示す図である。

図 13 (f) は、非スクランブルセクタのデータ構造を示す図である。

20 図 14 は、本発明に係る情報再生装置 500 の構成を示すブロック図である。

図 15 は、情報再生装置 500 に含まれる光ディスクドライブ 509 の構成を示すブロック図である。

図 16 は、情報再生装置 500 に含まれる AV デコードカード 507 の構成を示すブロック図である。

25 図 17 は、本発明に係る情報再生装置 800 の構成を示すブロック図である。

図 18 は、情報再生装置 800 に含まれる SCSI 制御回路内蔵 AV デコードカード 801 の構成を示すブロック図である。

図 19 は、本発明に係る情報再生装置 (光ディスクプレーヤ) 1000 の構成

を示すブロック図である。

図 20 は、デスクランブル回路 1106 の構成を示すブロック図である。

図 21 は、デスクランブル回路 1106 によって実行されるデスクランブル処理の手順を示すフローチャートである。

5 図 22 は、デスクランブル回路 1308 の構成を示すブロック図である。

図 23 は、デスクランブル回路 1308 によって実行されるデスクランブル処理の手順を示すフローチャートである。

図 24 は、デコーダ認証回路 601 の構成を示すブロック図である。

図 25 は、ドライブ認証回路 701 の構成を示すブロック図である。

10 図 26 は、光ディスクドライブ 509 と AV デコーダカード 507 又は SCSI 制御回路内蔵 AV デコーダカード 801 間の相互認証処理を説明するためのフローチャートである。

発明を実施するための最良の形態

15 以下、図面を参照しながら、本発明の実施の形態を説明する。

(第 1 の実施形態)

図 1 は、本発明に係る情報記録媒体のデータ構造を示す。以下、情報記録媒体としてディスクを例にとり説明する。しかし、本発明に係る情報記録媒体は、ディスクに限定されず、任意の情報記録媒体であり得る。

20 一般に、ディスク上で何らかの情報が記録されている情報記録領域は、主として制御情報が記録されるリードイン領域と、ユーザデータが記録されるデータ記録領域とに大別される。また、データ記録領域はセクタと呼ばれる単位で区切られているのが一般的である。ここで、ディスク再生装置は、リードイン領域を直接的にアクセスすることができるが、ディスク再生装置以外の装置（例えば、パーソナルコンピュータ）は、リードイン領域を直接的にアクセスすることができ
25 ない。

各セクタは、セクタを識別するためのセクタ ID (Identifier) 等が記録されるヘッダ領域と、ユーザデータが記録されるユーザデータ領域と、再生時の読み

出し誤りを訂正するための符号が記録されるECC (Error Correction Code) 領域とを含む。本実施の形態では、セクタ中のユーザデータ領域に記録されるユーザデータに対してスクランブル処理が施されているものとする。従って、情報再生装置が図1のディスクからユーザデータを正しく再生するためには、そのユーザデータに対して施されているスクランブル処理方法を知る必要がある。

図1のディスクのリードイン領域の所定の位置には、ユーザデータに対して施されているスクランブル処理方法を定める情報（以下、本明細書において「スクランブル情報」という）が記録されている。情報再生装置は、スクランブル情報が記録された領域を読み出し、そのスクランブル情報を解釈し、そのスクランブル情報に従った逆スクランブル処理をユーザデータに対して施す。これにより、ユーザデータを正しく再生することが可能となる。

ここで、一般に知られているスクランブル処理方法の一例を図9を用いて説明する。

図9(a)は、1つのセクタが、セクタID領域と、2048バイトのユーザデータ領域と、ECC領域とから成ることを示している。ユーザデータ領域には、データバイト列 $D_0, D_1, \dots, D_{2047}$ が記録される。データバイト列 $D_0, D_1, \dots, D_{2047}$ は、記録されるべき（スクランブル処理前の）データバイト列 $D'_0, D'_1, \dots, D'_{2047}$ と乱数系列 $S_0, S_1, \dots, S_{2047}$ との論理演算によって求められる。例えば、その論理演算は、排他的論理和であり得る。ここで、乱数系列 $S_0, S_1, \dots, S_{2047}$ は、与えられた初期値に対して一意に定まるものとする。

乱数系列 $S_0, S_1, \dots, S_{2047}$ の初期値を求めるために、セクタ中の所定ビット列（例えば、セクタID領域の所定位置の3ビット）に基づいて図9(b)に示すようなテーブルが参照される。例えば、セクタID領域の所定位置の3ビットが(0, 0, 1)である場合には、そのテーブルより初期値が100Fhと求まり、乱数系列 $B_0, B_1, \dots, B_{2047}$ ($S_0, S_1, \dots, S_{2047}$ に相当する) が一意に定まる。

与えられた初期値から乱数系列 $S_0, S_1, \dots, S_{2047}$ を発生する方法と

しては、例えば、図 9 (c) に示すようなシフトレジスタを用いる方法が知られている。

スクランブル処理方法としては、この他にも、ユーザデータのバイト列内で所定ビットを入れ替える等の他の方法を用いることも可能である。以下では、図 9
5 で述べたスクランブル処理方法を用いて、説明を行う。

図 2 は、図 1 に示されるディスクのリードイン領域の所定位置に記録されるスクランブル情報の構造を示す。

図 2 (a) に示されるように、この例では、スクランブル情報は、スクランブル処理に用いる乱数系列の初期値を得るテーブルを指定する識別子である。なお、
10 そのテーブル以外のスクランブル処理方法を特定するための情報はあらかじめ定義されているものとする。

例えば、スクランブル情報の内容が (1, 0) であることは、あらかじめ定義された図 2 (b) に示される 4 つのテーブルのうち、テーブル 2 がスクランブル処理に用いられたことを示す。情報再生装置は、図 2 (b) の 4 つのテーブルを
15 格納するメモリを有しており、スクランブル情報に応じて逆スクランブル処理に使用するテーブルを切り替える。これにより、ユーザデータに対する逆スクランブル処理を正しく実行することが可能となる。

図 3 は、本発明に係るディスクの他のデータ構造を示す。図 3 に示されるディスクのリードイン領域には、初期値テーブルが直接記録されている。そのディスク
20 のデータ記録領域には、その初期値テーブルを用いて発生された乱数系列によってスクランブル処理が施されたユーザデータが記録されている。ここで、図 3 に示したスクランブル処理方法が有する他のパラメータはあらかじめ一意に定められているものとする。

情報再生装置は、ディスクのリードイン領域に記録された初期値テーブルを読み出し、その初期値テーブルを解釈する。その後、情報再生装置は、初期値テーブルに従った逆スクランブル処理手順を設定し、その逆スクランブル処理手順に従ってユーザデータを逆スクランブルする。これによって、スクランブルされた
25 ユーザデータを正しく再生することができる。

また、ディスクをある特定の逆スクランブル処理手順しか有さない情報再生装置で再生することは、そのディスクの初期値テーブルと情報再生装置の初期値テーブルが一致する場合に限られ、それ以外の場合は正しく再生することは不可能となる。

5 なお、上述した実施の形態では、図9で示したスクランブル処理方法における乱数系列の初期値テーブルを変更する方法を示した。しかし、図9で示したスクランブル処理方法である必要はなく、全く異なるスクランブル処理方法を使用することも可能である。また、図9で示したスクランブル処理方法において、初期
10 値テーブルの他にも変更可能なパラメータは多様にあり（例えば初期値テーブルを参照するためのビット列の取り方や乱数を発生させるシフトレジスタの構成など）、変更可能なパラメータの各々や組み合わせに識別子を与えることも可能となる。

15 上述したように、本発明に係る情報記録媒体によれば、用途や複製許可／不許可に応じてスクランブル処理方法を変更することが可能となる。その結果、不正な再生（例えば業務用ディスクを民生用ディスク再生装置で再生すること）や不正なコピーを防止することができる。

（第2の実施形態）

20 図4は、本発明に係る情報再生装置の構成を示す。情報再生装置は、ホストコンピュータ1と、ディスク3に記録されたデータを再生するディスク再生装置2とを含んでいる。

25 ホストコンピュータ1は、インタフェース部（I/F部）4と、映像情報を表示可能な形式に復号するAVデコーダ6と、表示装置7に映像情報を送出するビデオボード8と、CPU10と、DRAM（Dynamic Random Access Memory）などの内部メモリ11とを含んでいる。ビデオボード8と、CPU10と、内部メモリ11とは、バス9を介して相互に接続される。ビデオボード8の出力は、表示装置（出力装置）7に接続されている。ハードディスクドライブ12は、インタフェース部4に接続されている。

ディスク再生装置 2 は、インタフェース部 5 と、ディスク 3 からデータを読み出すための機構・信号処理回路・制御回路等を含むデータ再生部 13 と、ディスク再生装置 2 を制御するマイクロプロセッサ 14 とを含んでいる。

5 ホストコンピュータ 1 とディスク再生装置 2 とは、インタフェース部 4、5 を介して接続されている。例えば、インタフェース部 4、5 は、SCSI (Small Computer System Interface) や ATAPI (AT Attachment Packet Interface) 等の既存のインタフェース又は独自に定義されたインタフェースによって接続され得る。

10 ディスク再生装置 2 は、ディスク再生装置 2 のリセット時やディスク 3 の交換時において、ディスク 3 のリードイン領域に記録されたスクランブル情報を読み出し、そのスクランブル情報を解釈し、そのスクランブル情報に従った逆スクランブル処理手順をデータ再生部 13 に設定する。

15 ホストコンピュータ 1 は、ディスク 3 のデータ記録領域に記録されたユーザデータを出力装置 7 に表示するために、ディスク再生装置 2 に対してインタフェース部 4、5 を介して再生専用コマンド (以下、Play AV コマンドと称する) を発行する。ディスク再生装置 2 は、Play AV コマンドに応答して、スクランブル情報に従って逆スクランブル処理が施されたユーザデータをホストコンピュータ 1 に送信する。

20 ホストコンピュータ 1 のインタフェース部 4 は、Play AV コマンドを使用してディスク再生装置 2 から受け取ったユーザデータはデータバス 9 には送らず、AV デコーダ 6 にのみ送る。従って、Play AV コマンドを用いて得られたユーザデータをホストコンピュータ 1 に接続されたハードディスクドライブ 12 等の書き換え可能媒体に記録することは不可能である。

25 ホストコンピュータ 1 は、ディスク 3 のデータ記録領域に記録されたユーザデータをハードディスク 12 や内部メモリ 11 に記録する必要がある場合には、データ読出しコマンド (以下、Read コマンドと称する) を発行する。ディスク再生装置 2 は、その Read コマンドに応答して、ディスク 3 のコピーが許可されているか否かをあらかじめ保持しているスクランブル情報をもとに判定する。

ディスク再生装置 2 は、スクランブル情報で指定されるスクランブル方式がコピー許可されたタイプであるか否かによって、異なる動作をする。

5 ディスク再生装置 2 がディスク 3 のコピーが許可されていると判定した場合には、ディスク再生装置 2 の立ち上げ動作時にディスク 3 のリードイン領域から読み込んだスクランブル情報に従って逆スクランブル処理を施した正しいユーザデータをホストコンピュータ 1 に送信する。一方、ディスク再生装置 2 がディスク 3 のコピーが禁止されていると判定した場合には、スクランブル情報とは異なる逆スクランブル処理を施した誤ったユーザデータをホストコンピュータ 1 に送信する。あるいは、エラー処理を行う等を行うことによって、ディスク再生装置 2
10 が正しいデータをホストコンピュータ 1 に返送しないようにしてもよい。このようにして、不法な複製を防止することが可能となる。

ディスク 3 のコピーが許可されているか否かを示す情報（コピー許可情報）を得る方法としては、様々な方法がある。例えば、コピー許可情報がディスク 3 の所定の領域に記録されている場合には、ディスク再生装置 2 がディスク 3 のその
15 所定の領域からコピー許可情報を読み出せばよい。あるいは、コピー許可情報に応じてスクランブル処理方式が限定されている場合には、読み出されたスクランブル情報によってコピー許可情報を特定することができる。

あるいは、コピー許可情報は、スクランブル情報の一部によって表され得る。例えば、スクランブル情報が複数のビットからなる場合において、その複数のビットのうち 1 ビットでコピー許可情報を表すことにしてもよい。このように、スクランブル情報は、コピーが許可されたデータに施すスクランブル方式と、コピーが禁止されたデータに施すスクランブル方式とを明確に区別するために使用され得る。従って、ディスク 3 からスクランブル情報を読み出すことにより、コピーが許可されているか否かを判定することが可能となる。以下、コピー許可情報は
25 スクランブル情報の一部によって表されるとして説明する。

図 5 は、本発明に係る情報再生装置の他の構成を示す。図 5 の情報再生装置では、図 4 のホストコンピュータ 1 において独立していた A V デコーダ 6 とインターフェース部 4 とが、一体化した構成となっている。その他の構成は、図 4 の情報

再生装置の構成と同様である。

Play AV コマンドがホストコンピュータ 1 から発行されると、スクランブル情報に従って逆スクランブル処理を施されたユーザデータがディスク再生装置 2 からホストコンピュータ 1 に送信される。そのユーザデータは、AV デコーダ 6 によって AV デコードされて、その後、ビデオボード 8 に直接入力される。他の動作については、図 4 を用いて説明した実施の形態の情報再生装置と同様であるため、説明を省略する。

図 6 は、本発明に係る情報再生装置の他の構成を示す。図 6 の情報再生装置は、AV デコーダ 6 と一体化したインタフェース部 4 b と、インタフェース部 4 b とは独立したインタフェース部 4 a とを含んでいる。その他の構成は、図 5 の情報再生装置と同様である。

AV デコーダ 6 内のインタフェース部 4 b からは Play AV コマンドのみが発行される。一方、Read コマンドは、インタフェース部 4 b とは独立したインタフェース部 4 a から発行される。他の動作については、図 4 を用いて説明した実施の形態の情報再生装置と同様であるため、説明を省略する。

図 7 は、本発明に係る情報再生装置の他の構成を示す。図 7 の情報再生装置では、データを表示可能な形式に変換する AV デコーダ 6 がディスク再生装置 2 に内蔵されている。従って、ディスク再生装置 2 をホストコンピュータ 1 に接続することは不要である。

以下に本構成の情報再生装置の動作を説明する。図 7 のディスク再生装置 2 において、マイクロプロセッサ 14 は、図 1 に示すディスクからスクランブル情報を読み出し、そのスクランブル情報を解釈し、そのスクランブル情報に従った逆スクランブル処理をユーザデータに施す。逆スクランブル処理が施されたユーザデータは AV デコーダに送られる。ユーザデータは、AV デコーダ 6 によって AV デコードされ、出力装置 7 に出力される。このようにしてディスク 3 に記録されたユーザデータの再生が可能となる。

しかしながら、ディスク再生装置 2 で再生することが好ましくないスクランブル情報がディスク 3 に記録されていた場合には、ディスク再生装置 2 は正しい再

生を行わないことも可能である。例えば、ディスク 3 がカラオケ用途に使用される業務用ディスクであると仮定する。この場合において、そのディスク 3 が民生用ディスク再生装置に装着された場合には、民生用ディスク再生装置がディスク 3 に記録されたデータの再生を行わないようにすることも可能である。民生用ディスク再生装置は、ディスク 3 に記録されたスクランブル情報から民生用ディスクには使用されないスクランブル処理方法であるか否かを判定することができるからである。このように、ディスク 3 の用途に応じて使用可能なスクランブル処理方法を限定することにより、ディスク再生装置 2 がスクランブル情報に基づいて、ディスク 3 に記録されたデータを再生すべきか否かを判定することが可能となる。

また、特定の逆スクランブル処理のみを行うことが可能なディスク再生装置に対して、その逆スクランブル処理に対応しないスクランブル処理方法でスクランブルされたデータを記録したディスクを製造することにより、そのディスク再生装置がそのディスクに記録されたデータを再生することを禁止することが可能となる。

図 8 は、本発明に係る情報再生装置の構成を示す。情報再生装置は、ホストコンピュータ 1 と、ディスク再生装置 11 とを含んでいる。ホストコンピュータ 1 は、図 8 には示されていない。ホストコンピュータ 1 の構成は、図 4 ～ 図 6 のホストコンピュータ 1 の構成と同様である。

ディスク再生装置 11 は、インタフェース部 (I/F 部) 5 と、ディスク 3 に記録されたデータを読み出すデータ再生部 13 と、ディスク再生装置 11 を制御するマイクロプロセッサ 14 と、逆スクランブル回路部 15 と、復調・エラー訂正部 16 と、マイクロプロセッサ 14 によって実行されるプログラム等を格納する ROM (Read Only Memory) 17 と、データ処理用 RAM (Random Access Memory) 20 とを含んでいる。インタフェース部 5 と、データ再生部 13 と、マイクロプロセッサ 14 と、逆スクランブル回路部 15 と、復調・エラー訂正部 16 と、データ処理用 RAM 20 とは、内部データバス 19 を介して相互に接続されている。逆スクランブル回路部 15 は、初期値テーブル格納用メモリ 18 を含ん

でいる。

マイクロプロセッサ14は、電源投入時やディスク3が交換された時等に、ディスク3からスクランブル情報を読み出し、そのスクランブル情報を解釈する。

5 ディスク3が図2に示すデータ構造を有する場合には、マイクロプロセッサ14は、ROM17に予め格納された複数の初期値テーブルの中から、スクランブル情報の内容に従って1つの初期値テーブルを選択する。マイクロプロセッサ14は、選択された初期値テーブルを逆スクランブル回路部15内の初期値テーブル格納用メモリ18に格納する。初期値テーブル格納用メモリ18は、例えば、RAMであり得る。あるいは、初期値テーブル格納用メモリ18がROMである
10 場合には、そのROMに複数の初期値テーブルを予め格納しておいてもよい。

 ホストコンピュータ1がPlay AVコマンドを発行すると、そのPlay AVコマンドは、ディスク再生装置2のインタフェース部5を介してマイクロプロセッサ14に入力される。マイクロプロセッサ14は、Play AVコマンドに
15 応答して、スクランブルされたユーザデータに対して逆スクランブル処理を行うように逆スクランブル回路部15に指示する。逆スクランブル回路部15は、初期値テーブル格納用メモリ18に格納された初期値テーブルに従って逆スクランブル処理を行う。逆スクランブル処理が施されたデータは、インタフェース部5を介してホストコンピュータ1に送信される。このようにして、ディスク3に記録されたデータを再生することが可能となる。

20 一方、ホストコンピュータ1がReadコマンドを発行すると、そのReadコマンドは、ディスク再生装置11のインタフェース部5を介してマイクロプロセッサ14に入力される。このとき、マイクロプロセッサ14は、ディスク3からあらかじめ読み出したスクランブル情報からコピーが許可されているスクランブル方式か否かを判定する。マイクロプロセッサ14は、コピーが禁止されていると判定した場合には、スクランブル情報に対応する初期値テーブルとは異なる
25 初期値テーブルを逆スクランブル回路部15に設定する。あるいは、マイクロプロセッサ14は、初期値テーブルを逆スクランブル回路部15に設定することなく、ホストコンピュータ1にエラーを返送するようにしてもよい。このようにし

て、ディスク 3 に記録されたデータが再生されることを防止することができる。

また、マイクロプロセッサ 14 がスクランブル情報からコピーが許可されていると判定した場合において、ディスク 3 が図 3 に示すデータ構造を有する場合には、マイクロプロセッサ 14 は、ディスク 3 のリードイン領域から初期値テーブルを読み出し、その初期値テーブルを逆スクランブル回路部 15 内の初期値テーブル格納用メモリ 18 に格納する。初期値テーブル格納用メモリ 18 は、書き込み可能なメモリ（例えば、RAM）である。その他の処理は、ディスク 3 が図 2 に示すデータ構造を有する場合と全く同様であるので、ここでは省略する。

上述したように、本発明に係る情報再生装置によれば、情報記録媒体に記録されたスクランブル情報に応じて逆スクランブル処理方法を変更することが可能となる。これにより、複数種類の異なるスクランブル処理方法でスクランブルされたデータを正しく再生することが可能となる。

また、本発明に係る情報再生装置によれば、情報記録媒体に記録されたスクランブル情報に応じて情報再生装置が情報記録媒体に記録されたデータを再生すべきか否かを判定することができる。その結果、不法な複製を防止し、情報記録媒体に記録されたデータの著作権を保護することができる。

（第 3 の実施形態）

図 10（a）は、本発明に係る情報記録媒体のデータ構造を示す。情報記録媒体上の何らかのデータが記録されている情報記録領域は、リードイン領域と、データ記録領域と、リードアウト領域とを含む。リードイン領域には、情報再生装置が情報記録媒体を再生するために必要とする情報が記録されている。データ記録領域には、主としてユーザにとって有用なプログラムデータや AV データ等のデータが記録されている。

図 10（b）は、リードイン領域に記録されているコントロールデータ領域のデータ構造を示す。コントロールデータ領域は、物理情報セクタと、スクランブル情報セクタとを含んでいる。物理情報セクタには、ディスク径やディスク構造、

記録密度等のディスクの物理情報が記録されている。スクランブル情報セクタには、情報記録媒体のデータ記録領域に記録されたデータに対して施されたスクランブル方式等の情報が記録されている。スクランブル情報セクタは、情報再生装置が逆スクランブル処理を施すために参照される。なお、スクランブル情報セクタの詳細な内容については、後に図を参照して説明する。

図10(c)は、ボリューム・ファイル管理領域のデータ構造を示す。本実施の形態では、ボリューム・ファイル管理領域のデータ構造は、国際標準規格ISO9660(International Standard Organization 9660)に準拠している。この国際標準規格ISO9660は、CD-ROM(Compact Disc-Read Only Memory)において採用されている。

ボリューム・ファイル管理領域は、ボリューム記述子と、パステーブルと、ディレクトリレコードとを含んでいる。

ボリューム記述子には、ボリューム空間のサイズやパステーブルの記録位置情報、ディレクトリレコードの記録位置情報、ディスク作成日時等の情報が記録されている。パステーブルには、情報記録媒体上に存在する全てのディレクトリのパスと記録位置情報とを対応づけるテーブルが記録されている。ディレクトリレコードには、各ディレクトリまたはファイルの識別子(一般的には、ディレクトリ名又はファイル名)、データの記録位置情報、ファイルのサイズ、属性等の情報が記録されている。

図10(d)は、ディレクトリレコードの更に詳細なデータ構造を示している。ルートディレクトリ用ディレクトリレコードには、ルートディレクトリの属性や識別子、作成日時等が記録されている。また、ルートディレクトリ用ディレクトリレコード(第1セクタ)には、ディレクトリの記録位置情報が記録されている。ルートディレクトリ用ディレクトリレコード(第2セクタ)にも、同様な情報が記録されている。また、ファイルA用ディレクトリレコードには、ファイルAのデータの記録位置情報、データ長、ファイルの識別子情報、著作権管理識別子等

が記録されている。このように、複数のディレクトリは階層構造を有している。ルートディレクトリは、その階層構造の最も上位に位置するディレクトリである。これらの更に詳細な内容については後に図を参照して説明する。

5 データ記録領域には、スクランブルされているファイルと、スクランブルされていないファイルとが記録されている。例えば、スクランブルファイルAとスクランブルファイルCとは、スクランブルされているファイルであり、非スクランブルファイルBは、スクランブルされていないファイルである。著作権保護の対象になっているAVデータを格納するファイルは、スクランブルされているファイルであることが好ましい。

10 図10(e)は、スクランブルファイルAのデータ構造を示す。ファイルAは、セクタnから連続する複数のセクタに区分されている。複数のセクタのそれぞれに格納されるデータには、スクランブル処理が施されている。以下、本明細書では、スクランブル処理が施されたデータを格納するセクタを「スクランブルセクタ」という。

15 図10(f)は、非スクランブルファイルBのデータ構造を示す。ファイルBは、セクタmから連続する複数のセクタに区分されている。複数のセクタのそれぞれに格納されるデータには、スクランブル処理は施されていない。以下、本明細書では、スクランブル処理が施されていないデータを格納するセクタを「非スクランブルセクタ」という。

20 図11(a)～(c)は、ボリューム・ファイル管理領域中のディレクトリレコードのデータ構造を示す。ディレクトリレコードは、ディレクトリレコード長と、ファイル記録位置情報と、ファイルデータ長と、ファイル識別子と、著作権管理情報とを含む。

25 ディレクトリレコード長は、ファイル(又はディレクトリ)のディレクトリレコードのサイズを示す情報である。ファイル記録位置情報は、ファイルのデータが記録されたセクタ(以下、エクステンと称す)の開始位置を示す情報である。

ファイルデータ長は、ファイルを構成するセクタ数を示す情報である。ファイル識別子は、ファイルを識別するための識別情報（ファイル名）である。著作権管理情報は、ファイルの著作権管理に関する情報である。

著作権管理情報は、スクランブルフラグ領域とスクランブル方式領域とを含む。

5 スクランブルフラグ領域には、ファイルのデータにスクランブル処理が施されているか否かを示すフラグが記録される。ファイルのデータにスクランブル処理が施されている場合には、値 1 を有するフラグがスクランブルフラグ領域に記録され、ファイルのデータにスクランブル処理が施されていない場合には、値 0 を有するフラグがスクランブルフラグ領域に記録される。従って、スクランブルフラグ領域を参照することにより、ファイルのデータにスクランブル処理が施されているか否かを判定することができる。スクランブル方式領域には、ファイルのデータに施されたスクランブル処理の方式を示す識別子が記録される。従って、スクランブル方式領域を参照することによって、データに施されたスクランブル処理方式をファイル単位に決定することができる。

10

15 以下、図 1 1（d）～（f）を参照して、スクランブル方式の一例を説明する。このスクランブル方式に対応するスクランブル方式識別子を 1 とする。

図 1 1（d）は、リードイン領域のコントロールデータ領域に記録されているスクランブル情報セクタのデータ構造を示す。スクランブル情報セクタは、セクタヘッダ領域とメインデータ領域とを含む。

20 スクランブル情報セクタのセクタヘッダ領域は、情報再生装置がセクタを識別するための識別子が記録されているアドレス領域と、情報記録領域に施されたスクランブル方式を特定するための情報（前記のように、本例のスクランブル方式を 1 とする）が記録されたスクランブル方式領域と、情報再生装置が再生データの転送を要求する機器に著作権保護対象のデータを送出して良いか否かを決定するための認証処理（以下、相互認証処理と呼ぶ）に使用する相互認証鍵が記録された相互認証鍵領域とを含む。この相互認証処理については後に詳しく述べる。

25

スクランブル情報セクタのメインデータ領域には、スクランブルのための鍵からスクランブル処理時に使用する乱数系列を決定するためテーブルが記録されている。従って、情報再生装置は、スクランブル情報セクタに記録されたテーブルとスクランブルのための鍵とを用いることで初めて、デスクランブル処理が可能となる。ただし、上記の乱数系列を決定する初期値を、以下ではプリセットデータと称する。

図 1 1 (e) は、データ記録領域中のスクランブルセクタのデータ構造を示す。

スクランブルセクタのセクタヘッダ領域は、アドレス領域と、セクタのメインデータ領域にスクランブル処理が施されているか否かを識別するフラグが記録されたスクランブルフラグ領域と、スクランブル時に使用した鍵（以下、シードキーと称す）が記録されたシードキー領域と、ファイルの用途を識別する情報が記録された用途識別情報領域とを含む。スクランブルフラグ領域には、スクランブル処理が施されていることを示す 1 が記録されており、シードキー領域にはメインデータ領域のデスクランブル処理に用いる鍵が記録されている。また、用途識別情報領域には、業務用、民生用等の記録されたデータの用途についての情報が記録されており、情報再生装置の用途が用途識別情報と異なる場合の再生制限を示す情報が記録されている。また、メインデータ領域には、リードイン領域のスクランブル情報セクタで指定されたスクランブル方式と、スクランブルセクタのセクタヘッダ領域のシードキーとによって決定されるスクランブル処理が施されたデータが記録されている。つまり、シードキー領域に記録された値をもとにスクランブル情報セクタのテーブルを参照してプリセットデータを決定し、そのプリセットデータによって決定される乱数系列を用いてスクランブル/デスクランブル処理が可能となる。以下では、シードキーはファイル毎に同一であるとして説明を行う。

一方、非スクランブルセクタのセクタヘッダは、アドレス領域とスクランブルフラグ領域を含む。スクランブルフラグ領域には、セクタのメインデータ領域に

スクランブル処理が施されていないことを示す0が記録されている。従って、情報再生装置は、スクランブルフラグ領域の値が0であることを検知することにより、デスクランブル処理を施す必要がないことを容易に認識できる。

次に、図12を参照して、スクランブル方式の一例を説明する。

5 図12(a)は、8ビットのデータ系列 D_j (j は0から2047までの整数)をある初期値をもとに発生させた8ビットの乱数系列 S_j と論理演算を行うことにより、スクランブルされたデータ SD_j が得られることを示す。すなわち、リードイン領域に記録されたスクランブル情報セクタと、各セクタのセクタヘッダ領域のシードキーによって定まる15ビットのプリセットデータをシフトレジスタ301にセットし、上位ビット方向にシフトを行いながら最上位ビット r_7 とビット r_0 の排他的論理和をビット0に入れることで乱数系列 S_j を発生する。ここで、1ビットシフトする度にビット位置 r_0 のビットを論理演算ブロック302に入力し、8回のシフトによって論理演算ブロック302に入力される8ビットの数値を S_j とする。以上の様にして得られる S_j と8ビットの記録データ D_j との論理演算(例えば、排他的論理和など)によってスクランブル後のデータ SD_j が得られる。1セクタのメインデータのサイズを2048バイトとすると、前記の操作を SD_0 から SD_{2047} まで2048回繰り返すことで1セクタのスクランブル処理を行うことができる。

10 15

また、図12(b)および(c)は、スクランブル情報セクタからプリセットデータを決定するテーブルへの変換を示している。図12(b)に示すスクランブル情報セクタには、テーブルの各エントリが4つ記録されており、各エントリはシードキーとプリセットデータの組から成る。これらの組をテーブル化すれば図12(c)の様なテーブルが得られる。例えば、セクタヘッダに記録されているシードキーが01b(bは2進数であることを意味する)であれば、プリセットデータとして0077h(hは16進数を意味する)を図12(a)のシフトレジスタ301に初期値として設定し、上記のシフト動作および論理演算を施す

20 25

ことで、スクランブル／デスクランブル処理が可能となる。

5 以上のように、本実施形態の情報記録媒体は、ファイル単位でスクランブルをかけることを可能とするとともに、スクランブルが施されているか否かの情報をファイル管理領域に著作権管理情報として有するとともに、セクタ単位にもセクタヘッダのスクランブルフラグ領域に有することで、パーソナルコンピュータのようにメインデータの認識しか行えない装置にスクランブル処理の有無の認識を可能とし、光ディスクドライブのようなメインデータの認識が行えない装置にもスクランブル処理の有無の認識を可能とする。従って、パーソナルコンピュータに接続された光ディスクドライブによってデータを再生する場合にも、その両者が著作権保護対象のデータであるか否かを判別することを可能とする。

10 また、本実施の形態の情報記録媒体は、シードキーを変更することによってファイル毎に異なるスクランブル処理を施すことができるため、仮に不正行為によって一つのスクランブルファイルのスクランブル方法を解読されたとしても、解読されたスクランブル方式で他のスクランブルファイルをデスクランブルすることを防止することができ、著作権保護処理を行う上でのセキュリティを向上することが可能となる。

15 また、本実施の形態の情報記録媒体を著作権保護目的で使用する場合には、デスクランブルに必要な不可欠なスクランブル情報を記録したスクランブル情報セクタが、パーソナルコンピュータのような機器からは読み出すことのできないリードイン領域に存在しているために、スクランブル情報を不正に読みだそうとする行為を防止する効果が高い。また、リードイン領域はデータ記録領域と同一の再生手段で再生可能なために、特別な再生手段を新たに設ける必要がない。

20 また、セクタ単位に記録した、シードキー、スクランブルフラグ、用途識別情報等の情報を、パーソナルコンピュータのような機器からは読み出すことのできないセクタヘッダ領域に記録しているために、前記のリードイン領域にスクランブル情報を記録するのと同様に、不正に前記情報を読み出そうとする行為を防止

する効果がある。

また、セクタヘッダ領域に用途識別情報を記録しているために、記録されたデータの内容に応じて再生装置が再生を行うべきか、再生を禁止すべきかの判定を行うことを可能とする。よって、例えば、業務用のディスクと民生用のディスク
5 とで本領域に異なる識別子を記録することで、民生用再生装置で業務用ディスクが再生することを防止できる。

また、相互認証処理に用いる相互認証鍵を記録することで、再生装置が相互認証動作で送受信するデータを該相互認証鍵毎に変更することが可能となり、相互
10 認証処理の処理方法を不当に解読することを防止する効果がある。従って、相互認証処理を不当に行って、磁気ディスクドライブなどに不当にコピー動作を行おうとする行為を防止することが可能となる。

なお、本実施の形態において、ボリューム・ファイル構造は国際規格である ISO 9660 をもとにしたが、本発明に述べたような情報を有するボリューム・
15 ファイル構造であればこれに限らないことは言うまでもない。

なお、本実施の形態において、スクランブル方式は乱数とデータの論理演算を用いるとしたが、本実施の形態のようにテーブルとテーブルを参照するためのシードキーを有するスクランブル方式であればこれに限らないことは言うまでもない。
20

なお、本実施の形態において、リードイン領域にはプリセットデータを決定するためのテーブルを記録したが、テーブルを決定するためのパラメータであればこれに限らず、あらかじめ既知の複数のテーブルからただ一つのテーブルを特定するための識別子を記録しても良い。

なお、本実施の形態において、スクランブルセクタのセクタヘッダ領域に用途識別情報領域として用途識別のための情報記録領域を確保したが、明確に分離した領域として確保しなくても、シードキーの値によって用途を分類するようにしても良いことは言うまでもない。
25

なお、本実施の形態において、スクランブルセクタはメインデータ領域の2048バイト全てにスクランブル処理が施されていることとしたが、メインデータ領域の全てにスクランブル処理が施されていなくとも、定められた一部の領域のみにスクランブル処理が施されていても良い。

5

(第4の実施形態)

次に、本発明に係る情報記録媒体の他のデータ構造を説明する。情報記録媒体のデータ構造は、図10に示される情報記録媒体の構造と同様である。ここでは、図10に示されるデータ構造と異なる点についてのみ説明する。

10 図13(a)～(c)は、ボリューム・ファイル管理領域に記録されたディレクトリレコードのデータ構造を示す。ディレクトリレコードの著作権管理情報中のスクランブル方式領域には、本実施の形態で説明するスクランブル方式を示す2が記録されている。

15 図13(e)は、スクランブルセクタのデータ構造を示している。スクランブルセクタのセクタヘッダ領域は、アドレス領域と、スクランブルフラグ領域と、メディアCGMS(Copy Generation Management System)データ領域と、暗号化オリジナルCGMSデータ領域と、暗号化タイトル鍵領域と、暗号化用途識別情報領域とを含む。

20 スクランブルフラグ領域には、スクランブル処理が施されていることを示す1が記録されている。

25 メディアCGMSデータ領域には、情報記録媒体のコピー許可情報が記録されている。暗号化オリジナルCGMSデータ領域には、本セクタのデータが他の媒体からコピーされている場合において、最もオリジナルのデータのコピー許可情報が記録されている。ここで、メディアCGMSデータは、情報記録媒体のデータのコピー許可情報を表す。メディアCGMSデータは、コピー動作時に更新される。オリジナルCGMSデータは、ディスク作成時のコピー許可情報を表す。

オリジナルCGMSデータは、暗号化が施されているために、コピー動作時もそのままコピーされる。(表1)にメディアCGMSデータ、オリジナルCGMSデータの定義を示す。

表 1

メディアCGMSデータ/ オリジナルCGMSデータ	内容
0 0 b	コピー許可
0 1 b	未使用
1 0 b	1回コピーのみ許可
1 1 b	コピー禁止

(表1)から、例えば、メディアCGMSデータが1 1 bであって、オリジナルCGMSデータが1 0 bであったとすれば、そのセクタのデータは、もともと1回のみコピー許可状態(メディアCGMSデータおよびオリジナルCGMSデータがともに0 1 b)であって、既に1回のコピー動作が行われたことによってメディアCGMSデータがコピー禁止を意味する1 1 bに変更されたと判定すべきである。以下では、メディアCGMSデータと、オリジナルCGMSデータを合わせてCGMS制御情報と称する。

暗号化タイトル鍵領域には、メインデータ領域に施されたスクランブル処理をデスクランブルするための鍵が記録されている。

暗号化用途識別情報領域には、用途を指定するための識別情報が暗号化されて記録されている。ただし、前記の暗号化オリジナルCGMSデータ領域、暗号化タイトル鍵領域、暗号化用途識別情報領域はいずれも暗号化処理が施されており、セクタヘッダ領域を読み出しただけでは情報を得ることはできない。これらの暗号化データは情報記録媒体のリードイン領域のセクタヘッダ領域に記録された暗号化ディスク鍵を用いて暗号化されている。したがって、スクランブル情報セク

タのヘッダ領域の暗号化情報を復号するためには、前記暗号化ディスク鍵が必要となる。

図13(d)は、スクランブル情報セクタのデータ構造を示す。以下の説明では、暗号化されたデータと暗号を復号化したデータとを明確に区別するため、暗号化されたデータは「暗号化」をつけた名称で表すこととし、暗号を復号化したデータは「復号化」をつけた名称で表すこととする。例えば、タイトル鍵を暗号化することによって得られるデータは「暗号化タイトル鍵」といい、暗号化タイトル鍵を復号化することによって得られるデータは「復号化タイトル鍵」という。

スクランブル情報セクタは、リードイン領域のコントロールデータ領域に記録されている。

スクランブル情報セクタのセクタヘッダ領域には、スクランブル方式が本方式のスクランブル方式であることを示す2が記録されている。また、相互認証鍵領域には、デスクランブル後のデータを送出するか否かを決定するための相互認証処理に用いられる相互認証鍵が記録されている。本相互認証鍵については、後述する情報再生装置の実施形態において、詳しく述べることとする。

スクランブル情報セクタのメインデータ領域には、スクランブルセクタの暗号化オリジナルCGMSデータ、暗号化タイトル鍵、暗号化用途識別情報を復号するための暗号化ディスク鍵が記録されている。ただし、暗号化ディスク鍵はさらに暗号化が施されており、暗号化ディスク鍵を復号するための鍵（以下、マスター鍵と称す）は、情報再生装置によって提供される。

スクランブル情報セクタのメインデータ領域には、暗号化ディスク鍵1、暗号化ディスク鍵2、・・・と複数の暗号化ディスク鍵が記録されており、暗号化ディスク鍵1はマスター鍵1で、暗号化ディスク鍵2はマスター鍵2で、・・・というようにそれぞれ対応したマスター鍵によって暗号化されている。ここで、暗号化ディスク鍵1、暗号化ディスク鍵2、・・・は、同一のディスク鍵情報を異なるマスター鍵で暗号化したものである。従って、ある情報再生装置Aがマスタ

一鍵 1 を内部に有しており、別の情報再生装置 B がマスター鍵 2 を内部に有している場合、情報再生装置 A は暗号化ディスク鍵 1 を、情報再生装置 B は暗号化ディスク鍵 2 をそれぞれ復号して、同一の内容の復号化ディスク鍵を得ることが可能となる。

- 5 図 1 3 (f) は、非スクランブルセクタのデータ構造を示す。スクランブルセクタフラグ領域には 0 が記録されている。メインデータ領域に記録されているデータにはスクランブル処理が施されていない。このことは、従来の情報記録ディスクと同様なデータアクセスが可能であることを示している。

- 10 以上のように、本実施形態の情報記録媒体は、非スクランブルセクタの再生に際しては従来と全く同様のアクセスでのデータ再生が可能である。一方、スクランブルセクタの再生を行うためには、マスター鍵を有する情報再生装置が、リードイン領域のスクランブル情報セクタを読み出して暗号化ディスク鍵をマスター鍵で復号し、さらに、復号化したディスク鍵を用いてスクランブルセクタのセクタヘッダの暗号化タイトル鍵を復号化し、復号化したタイトル鍵を用いてスクランブルデータのデスクランブル処理を行うことでデータの再生が可能となる。

- 15 以下では、スクランブル方式の例として、第 3 の実施形態で述べたスクランブル方式を用いる場合について述べる。第 3 の実施形態においては、変換テーブルを用いてプリセットデータを生成したが、本実施形態の情報記録媒体では、暗号化タイトル鍵領域に乱数発生のための初期値を暗号化して記録すれば、図 1 2 (a) のシフトレジスタ 3 0 1 と論理演算ブロック 3 0 2 とを用いて容易にデータのスクランブル処理が行える。すなわち、復号したタイトル鍵をシフトレジスタ 3 0 2 の初期値とし、シフトを繰り返すことで乱数系列 S_i を発生し、データ系列 D_i との論理演算をとることにより、スクランブル処理が可能となる。また、図 1 2 (a) のシフトレジスタ 3 0 1 を用いて、データのデスクランブルも同様に可能となる。

25 以上のように、本実施の形態の情報記録媒体は、ファイル単位でスクランブル

をかけることを可能とするとともに、スクランブルが施されているか否かの情報をファイル管理領域に著作権管理情報として有するとともに、セクタ単位にもセクタヘッダのスクランブルフラグ領域に有することで、パーソナルコンピュータのようにメインデータの認識しか行えない装置にスクランブル処理の有無の認識を可能とし、光ディスクドライブのようなメインデータの認識が行えない装置にもスクランブル処理の有無の認識を可能とする。従って、パーソナルコンピュータに接続された光ディスクドライブによってデータを再生する場合にも、その両者が著作権保護対象のデータであるか否かを判別することを可能とする。

また、本実施の形態の情報記録媒体は、タイトル鍵を変更することによってファイル毎に異なるスクランブル処理を施すことができるため、仮に不正行為によって一つのスクランブルファイルのスクランブル方式を解読されたとしても、解読されたスクランブル方式で他のスクランブルファイルをデスクランブルすることを防止することができ、著作権保護処理を行う上でのセキュリティを向上することが可能となる。

また、本実施の形態の情報記録媒体を著作権保護目的で使用する場合には、デスクランブルに必要な不可欠なスクランブル情報を記録したスクランブル情報セクタが、パーソナルコンピュータのような機器からは読み出すことのできないリードイン領域に存在しているために、スクランブル情報を不正に読みだそうとする行為を防止する効果が高い。また、リードイン領域はデータ記録領域と同一の再生手段で再生可能なために、特別な再生手段を新たに設ける必要がない。

また、セクタ単位に記録した、スクランブルフラグ、CGMS制御情報、暗号化タイトル鍵、暗号化用途識別情報を、パーソナルコンピュータのような機器からは読み出すことのできないセクタヘッダ領域に記録しているために、前記のリードイン領域にスクランブル情報を記録するのと同様に、不正に前記セクタヘッダ中の情報を読み出そうとする行為を防止する効果がある。

また、セクタヘッダ領域に用途識別情報を記録しているために、記録されたデ

ータの内容に応じて再生装置が再生を行うべきか、再生を禁止すべきかの判定を行うことを可能とする。よって、例えば、業務用のディスクと民生用のディスクとで本領域に異なる識別子を記録することで、民生用再生装置で業務用ディスクが再生することを防止できる。

- 5 また、相互認証処理に用いる相互認証鍵を記録することで、再生装置が相互認証動作で送受信するデータを該相互認証鍵毎に変更することが可能となり、相互認証処理の処理方法を不当に解読することを防止する効果がある。従って、相互認証処理を不当に行って、磁気ディスクドライブなどに不当にコピー動作を行おうとする行為を防止することが可能となる。

- 10 また、本実施の形態の情報記録媒体は、スクランブルセクタのメインデータをタイトル鍵で暗号化し、タイトル鍵をディスク鍵で暗号化し、ディスク鍵をマスター鍵で暗号化するという階層的な暗号化／スクランブル処理を施しているために、不正にスクランブルセクタのメインデータをコピーされた場合でも、そのデ
15 スクランブルを防止する効果があるため、不正コピーを無意味なものとする事が可能である。

 また、CGMS制御情報を記録しているために、本実施の形態の情報記録媒体から他の書き換え型媒体にファイルコピーされた場合にも、不正コピーされたか、正規コピーされたかを判定することを可能とする。

- 20 なお、本実施の形態ではタイトル鍵を初期値とした乱数とデータとの論理演算によってスクランブル処理を行う例を示したが、スクランブル方式はこれに限らず、指定された鍵に応じてデータをスクランブルする方式であれば他のスクランブル方式でも良いことは言うまでもない。

- なお、本実施の形態のボリューム・ファイル構造は、国際標準規格であるISO 9660をもとに説明したが、本実施の形態で述べた内容と同等の著作権管理
25 情報を記録できるボリューム・ファイル構造であれば、これに限らないことは言うまでもない。

なお、本実施の形態において、スクランブルセクタはセクタの全てのデータがスクランブルされているとしたが、セクタのメインデータ全域がスクランブルされていなくとも、メインデータの一部のみがスクランブルされていても良いことは言うまでもない。

- 5 なお、本実施の形態において、スクランブルファイルではファイルを構成する全てのセクタにスクランブルが処理が施されているとしたが、スクランブルファイルの一部のセクタのみにスクランブル処理が施されていても良いことは言うまでもない。

- 10 なお、本実施の形態において、CGMS制御情報は、1回コピーのみ許可、コピー禁止、コピー許可の3種のみを用いていたが、割り当てるビットを拡張することで容易に2回コピー許可、3回コピー許可などの情報を記録できることは言うまでもない。

- 15 なお、本実施の形態で述べたメインデータのスクランブル方法は一例であり、ある鍵情報（本実施の形態ではタイトル鍵）をもとにスクランブルする方法であれば、これに限らない。

（第5の実施形態）

- 20 以下、図面を参照しながら、本発明に係る情報記録媒体を再生するための情報再生装置を説明する。特に断らない限り、情報再生装置は、本発明に係る情報記録媒体の第3の実施の形態と第4の実施の形態に共通して再生可能な装置であることとする。従って、以下では情報記録媒体の第4の実施の形態を再生する場合の動作を例に説明するが、暗号化タイトル鍵領域をシードキー領域と、スクランブル情報セクタの暗号化ディスク鍵をプリセットデータ変換テーブルと、それぞれ置き換えることによって情報記録媒体の第3の実施の形態についても同様に処理できる。
- 25

図14は、本発明に係る情報再生装置500の構成を示すブロック図である。

情報再生装置 500 は、メインプロセッサ 501 と、バスインタフェース回路 503 と、主記憶 504 と、SCSI (Small Computer System Interface) で定められるプロトコルを制御する SCSI 制御カード 506 と、圧縮されたデジタル AV データを伸張してアナログ AV データに変換して出力する AV デコーダカード 507 と、本発明に係る情報記録媒体を再生する光ディスクドライブ 509 と、ハードディスクドライブ 510 とを含んでいる。

メインプロセッサ 501 と、バスインタフェース回路 503 と、主記憶 504 とは、プロセッサバス 502 を介して相互に接続されている。バスインタフェース回路 503 と、SCSI 制御カード 506 と、AV デコーダカード 507 とは、システムバス 505 を介して、相互に接続されている。SCSI 制御カード 506 と、光ディスクドライブ 509 と、ハードディスクドライブ 510 とは、SCSI バスを介して、相互に接続されている。

次に、情報再生装置 500 による AV ファイルの再生動作について説明する。

光ディスクドライブ 509 に光ディスクが装着されると、メインプロセッサ 501 は、SCSI 制御カード 506 を介して前記光ディスクのボリューム・ファイル管理領域を読み出し、主記憶 504 に格納する（以下、格納したボリューム・ファイル管理領域のデータをファイル管理情報と称す）。

メインプロセッサ 501 は、AV デコーダカード 507 と光ディスクドライブ 509 との間で互いの機器が著作権保護機能を有する機器であるか否かを判定する処理（以下、相互認証処理と称す）を行う。その処理過程においていずれかの機器からエラーを検出した場合には相互認証処理が失敗したとみなし、以下の処理を中止する。一方、相互認証処理が正常に終了した場合に光ディスクドライブ 509 は、装着されたディスクの暗号化ディスク鍵を AV デコーダカードに転送する。この際、光ディスクドライブ 509 は、暗号化ディスク鍵の出力時に、さらに相互認証処理中に生成した鍵（以下、バス鍵と称す）に基づいて暗号化を施した暗号化ディスク鍵を送出する。AV デコーダカード 507 は受け取った暗号

化ディスク鍵を、バス鍵で復号化を行った後、内部で保持する。

その後、光ディスクに記録されたファイルを再生する場合にメインプロセッサ 501は、あらかじめ主記憶504に格納したファイル管理情報中の著作権管理情報のスクランブルフラグを参照し、再生を行うファイルがスクランブルされた
5 ファイルであるか否かを判定する。判定の結果、再生するファイルがスクランブルされていないファイルであると判定されれば、光ディスクドライブ509はメインプロセッサ501からSCSI制御カード506を介して再生命令を受領し、非スクランブルデータを転送する。一方、メインプロセッサ501がファイル管理情報のスクランブルフラグからスクランブルされたファイルであると判定すれ
10 ば、再び光ディスクドライブ509とAVデコーダカード507間の相互認証処理を実行する。

メインプロセッサ501は、相互認証処理中にエラーを検出すれば、再生処理を行わずに処理を中止する。一方、相互認証処理が正常に終了した場合には、データの再生に先だって、光ディスクドライブ509は暗号化タイトル鍵を返送し、
15 メインプロセッサ501によってAVデコーダカード507に転送される。この時、光ディスクドライブ509はあらかじめ保持しているバス鍵によって暗号化した暗号化タイトル鍵を転送する。また、AVデコーダカード507は受け取った暗号化タイトル鍵を、バス鍵で復号化した後に内部的に格納する。

その後、光ディスクドライブ509は装着されたディスクから読み出されるスクランブルデータを送出し、マイクロプロセッサ501は該スクランブルデータをAVデコーダカード507に転送する。AVデコーダカード507は、既に内部に格納するタイトル鍵に用いて、受信したスクランブルデータをデスクランブルし、アナログAVデータに変換し、ビデオ出力、オーディオ出力からアナログ信号として出力する。以上のようにして、情報再生装置500は、本発明の情報
20 記録媒体を再生することが可能となる。

光ディスクドライブ509からハードディスクドライブ510へのスクランブ

ルファイルのコピー動作については、ハードディスクドライブ 510 が相互認証処理を実行できないために、相互認証処理がエラー終了となる。従って、光ディスクドライブ 509 がデータを SCSI バスに送出する前に処理は中止され、コピー動作は実行されない。

5 また、仮に、光ディスクドライブ 509 が読み出したスクランブルファイルを不当にハードディスクドライブ 510 へコピーするためのプログラムが主記憶 504 にロードされ、何らかの形で相互認証処理を正常終了させた後に、転送されたスクランブルデータをハードディスクドライブ 510 にコピーした場合には、スクランブルデータはハードディスクドライブ 510 にコピーされる。しかしながら、ハードディスクドライブ 510 にコピーされたデータを再生するためには、
10 再びハードディスク 510 と AV デコーダカード 507 の相互認証処理が必要となり、この場合にハードディスクドライブ 510 はバス鍵を生成する手段を持たないために、ハードディスク 510 上のスクランブルファイルが AV デコーダカード 507 によって再生されることは不可能となる。

15 従って、不正なコピーが仮になされたとしても、そのコピー動作を無意味なものとすることができ、結果として著作権保護機構を実現することができる。

以下に、情報再生装置 500 の構成要素である光ディスクドライブ 509 および AV デコーダカード 507 の更に詳細な構成および動作について、それぞれ図 15、図 16 を参照して説明する。

20 図 15 は、光ディスクドライブ 509 の構成を示すブロック図である。以下にその構成について説明する。600 は SCSI 制御回路を、601 は AV デコーダとの相互認証処理を行うためのデコーダ認証回路を、602 は光ディスクドライブ全体を制御するマイクロコントローラを、603 はマイクロコントローラの動作プログラムを格納したプログラム ROM を、604 は制御データを伝送する
25 制御バスを、605 はデータの再生時に、読み出しエラーを訂正するためのエラー訂正処理時に使用される ECC (Error Correction Code) 処理用メモリを、

606は光ディスク607からのデータの読み出し、2値化、復調、エラー訂正処理等を行うデータ再生回路を、607は本発明に係る情報記録媒体であって、前記第3の実施の形態又は第4の実施の形態に示されるデータ構造を有する光ディスクを、それぞれ示している。

- 5 次に、光ディスクドライブ509の動作について、相互認証処理時およびデータ再生時の動作について述べる。

相互認証処理要求をSCSI制御回路600によって受け取った光ディスクドライブ509は、デコード認証回路601を制御して定められた相互認証処理を実行する。本プロトコルについては、後に詳しく述べるためここでは省略する。

- 10 前記相互認証処理のプロトコルにおいて、マイクロコントローラ602が何らかのエラーを検出した場合には、SCSI制御回路600からエラーを報告して相互認証処理およびそれに続く鍵情報転送動作を中止する。正常に相互認証処理が終了した場合には、デコード認証回路601には相互認証処理時に決定されるバス鍵が格納される。

- 15 相互認証処理がディスク交換時やリセット時のものであれば、相互認証処理に引き続いて暗号化ディスク鍵の読み出し要求が光ディスクドライブ509に発行される。この時、光ディスクドライブ509は、データ再生回路606を制御して光ディスク607から暗号化ディスク鍵情報を読み出し、さらにデコード認証回路601で既に保持しているバス鍵を使用して暗号化を施した暗号化ディスク
- 20 鍵をSCSI制御回路600から送出する。一方、スクランブルファイルの再生時における相互認証処理であった場合は、相互認証処理の正常終了に引き続いて、暗号化タイトル鍵の読み出し命令を光ディスクドライブ509は受領する。この時光ディスクドライブ509は、データ再生回路606を制御して光ディスク607から暗号化タイトル鍵情報を読み出し、さらにデコード認証回路601で既に保持しているバス鍵を使用して暗号化を施したデータをSCSI制御回路600から送出する。
- 25

その後発行されるファイルデータの再生要求に対して光ディスクドライブ 509 は、光ディスク 607 から読み出したスクランブルデータを SCSI 制御回路 600 から送出する。以上で光ディスクドライブ 509 の説明を終わる。

5 なお、本実施の形態の光ディスクドライブ 509 は、暗号化ディスク鍵の転送要求を受領してから、光ディスク 607 の暗号化ディスク鍵領域を再生するとしたが、光ディスク 607 装着時に読み込んで、内部的に保持していても良いことは言うまでもない。

次に、AV デコーダボードの構成および動作について図 16 を参照して説明する。

10 図 16 は、AV デコーダカード 507 の構成を示すブロック図である。以下にその構成要素について説明する。700 はシステムバスと情報の送受信を制御するシステムインタフェース回路を、701 は光ディスクドライブ 509 と相互認証処理を行うドライブ認証回路を、702 は AV デコーダカード 507 全体を制御するマイクロコントローラを、703 はマイクロコントローラ 702 の動作プログラムを格納したプログラム ROM を、704 は制御情報を伝送する制御バスを、705 はスクランブルデータをデスクランブルするためのデスクランブル回路を、706 は圧縮されたデジタル AV データを伸張してアナログ AV データに変換するオーディオ/ビデオデコード回路を、707 はオーディオ/ビデオデコード回路 706 がデータ変換に使用する作業用メモリであるオーディオ/ビデオデコード用メモリを、それぞれ示している。

15 20

次に AV デコーダカード 507 の動作について、相互認証処理時およびスクランブルファイル再生時の動作について説明する。

まずリセット時やメディア交換時における相互認証処理時には、マイクロコントローラ 702 はドライブ認証回路 701 を制御して光ディスクドライブ 509 と所定のプロトコルに従って相互認証処理を実行する。前記相互認証処理中にドライブ認証回路 701 が何らかのエラーを検出した場合には、システムインタフ

25

エース回路700を介してエラーを報告し、処理を打ち切る。一方、正常に相互認証処理が終了した場合にドライブ認証回路701は相互認証処理で決定したバス鍵を内部的に保持する。

5 さらに、AVデコーダカード507は、システムインタフェース回路700から暗号化ディスク鍵を受け取る。ここで、受領した暗号化ディスク鍵は光ディスクドライブ509においてバス鍵を用いて暗号化されているため、AVデコーダカード507はドライブ認証回路701において既に保持するバス鍵で復号化した後にデスクランブル回路705に転送する。デスクランブル回路705内は受け取った暗号化ディスク鍵を、内部に格納する。

10 一方、スクランブルファイルの再生時には、ファイルの再生に先だって再び光ディスクドライブ509との相互認証処理が実行される。ここでも相互認証処理においてエラーが発生した場合には相互認証処理およびそれに続くファイル再生動作を中止する。相互認証処理がエラーなく正常に終了した場合にAVデコーダカード507は、システムインタフェース回路700を介して暗号化タイトル鍵を受信する。暗号化タイトル鍵は光ディスクドライブ509において、バス鍵を用いて更に暗号化されているために、ドライブ認証回路701において保持しているバス鍵によって復号され、デスクランブル回路705に転送される。デスクランブル回路705内は、受領した暗号化タイトル鍵を内部的に格納する。

15 その後、システムインタフェース回路700から受信するスクランブルファイルのスクランブルデータはそのままデスクランブル回路705に転送され、既に保持しているタイトル鍵をもとにデスクランブル処理が行われ、オーディオ/ビデオデコード回路706に転送されてアナログAV信号に変換されて出力される。

20 以上のように、本実施の形態の情報再生装置500によれば、内部の光ディスクドライブ509にデコーダ認証回路601、AVデコーダカード507にドライブ認証回路701をそれぞれ有しているために、ファイルを不正にコピーする
25 目的の機器には鍵情報を送出不し。したがって、仮にスクランブルファイルの

データが不正にコピーされたとしても、そのデスクランブルを実行するための鍵情報を送出しないことで、コピーデータを無意味なものとすることができる。従って、ファイルの著作権を保護する効果がある。

5 また、本実施の形態の情報再生装置によれば、A Vデコーダカード5 0 7内に鍵情報に応じたデスクランブル処理を施すデスクランブル回路7 0 5を有するために、スクランブルされたデータをデスクランブルして再生することが可能である。

10 なお、本実施の形態では、光ディスクドライブ5 0 9が接続されるバスをS C S Iバスであるとしたが、定められたプロトコルに従って再生データが転送できればこれに限らず、A T A P I (AT Attachment Packet Interface) やI E E E 1 3 9 4 (Institute of Electrical and Electronics Engineers 1394) 等に従ったバスであっても良いことは言うまでもない。

15 なお、本実施の形態において、デコーダ認証回路6 0 1の機能およびドライブ認証回路7 0 1の機能は、マイクロコントローラ6 0 2および7 0 2によって実行されるソフトウェアによって実現されてもよい。

(第6の実施形態)

次に、本発明に係る情報再生装置8 0 0を説明する。

20 図1 7は、本発明に係る情報再生装置8 0 0の構成を示すブロック図である。情報再生装置8 0 0の構成は、A Vデコーダカード8 0 1がS C S I方式に従って通信を行うためのS C S I制御回路を内蔵している点を除いて、図1 4に示す情報再生装置5 0 0の構成と同様である。従って、同一の構成要素には同一の参照番号を付し、その説明を省略する。

次に、情報再生装置8 0 0の動作を説明する。

25 S C S I制御回路内蔵A Vデコーダカード8 0 1は内部にS C S I制御回路を内蔵しているため、メインプロセッサ5 0 1から光ディスクドライブ5 0 9のス

クランブルファイル再生要求が発行されると、SCSI制御回路内蔵AVデコーダカード801と光ディスクドライブ509との間で相互認証処理が直接実行される。すなわち、SCSI制御回路内蔵AVデコーダカード801が光ディスクドライブ509に相互認証のためのコマンドシーケンスを発行し、光ディスクドライブ509がそのコマンドに応答することで相互認証処理を行う。

また、データの再生動作においても同様に、光ディスクドライブ509に再生要求を行うのは、SCSI制御回路内蔵AVデコーダカード801であって、メインプロセッサ501ではない。従って、光ディスクドライブ509が読み出したデータは直接SCSI制御回路内蔵AVデコーダカード801に入力され、アナログAV信号に変換されて出力される。

図18は、SCSI制御回路内蔵AVデコーダカード801の構成を示すブロック図である。以下では、図16に示したAVデコーダカード507の構成と異なる点についてのみ説明する。

900はSCSIバスとの送受信を制御するSCSI制御回路を、901はマイクロコントローラによって実行されるプログラムを格納したプログラムROMを、それぞれ示している。

システムインタフェース回路700にスクランブルファイルの再生要求が入力されれば、マイクロコントローラ702はドライブ認証回路701およびSCSI制御回路900を制御して、光ディスクドライブ509との相互認証処理を実行する。このとき、相互認証プロトコルは、光ディスクドライブ509に対してSCSI制御回路900から直接コマンドが発行される。また、マイクロコントローラ702は相互認証プロトコルに従ってドライブ認証回路701を制御して相互認証処理を行う。以上の相互認証処理がエラーで終了した場合には、マイクロコントローラ702はシステムインタフェース回路700を制御して、メインプロセッサ501にエラーを報告して処理を終了する。一方、相互認証処理が正常に終了した場合には、光ディスクドライブ509から直接SCSI制御回路9

報記録媒体の第4の実施の形態をもとに説明する。

光ディスクプレーヤ1000のリセット時又はディスク挿入時に、マイクロコントローラ702は、データ再生回路606を制御して、光ディスクのリードイン領域のスクランブル情報セクタの読み出しを行う。スクランブル情報セクタから読み出された暗号化ディスク鍵情報はデスクランブル回路705に転送されて、内部的に保持される。

一方、光ディスク607に記録されたスクランブルファイルを再生する際に、マイクロコントローラ702はデータ再生回路606を制御して、再生するスクランブルファイルのセクタヘッダ領域から暗号化タイトル鍵を読み出し、デスクランブル回路705に転送する。デスクランブル回路705は受け取ったタイトル鍵を内部に格納するとともに、用途識別情報の判定を行う。デスクランブル回路705は、用途識別情報を判定した結果、再生が禁止されていると判定した場合には、マイクロコントローラ702にエラーの発生を報告する。一方、デスクランブル回路705が再生が許可されていると判定した場合には、データ再生回路606はスクランブルファイルのデータを読み出し、読み出したスクランブルデータをデスクランブル回路705に転送する。デスクランブル回路705は、あらかじめ格納したディスク鍵およびタイトル鍵を用いてスクランブルデータをデスクランブルし、オーディオ/ビデオデコード回路706に転送する。オーディオ/ビデオデコード回路706は受け取ったデータをアナログAV信号に変換して、音声出力/映像出力する。

以上のようにして、光ディスクプレーヤ1000は、スクランブルデータをデスクランブルして再生することが可能である。ただし、本発明に係る情報再生装置の第5および第6の実施の形態とは異なり、光ディスクプレーヤ1000は相互認証処理を実行せずに映像再生を行う。これは、本実施の形態においては、再生されたデータが直接オーディオ/ビデオデコード回路706に入力されるため、途中でハードディスクドライブなどの他の書き換え型メディアへのコピー動作が

00によってスクランブルファイルのデータを受け取り、デスクランブル回路705でデスクランブルしたデータをオーディオ/ビデオデコード回路706でアナログAV信号に変換して出力する。以上により、第5の実施の形態の情報再生装置と同様に、本発明の情報記録媒体に記録されたデータの著作権を侵害するコピー動作を防止して、AVデータを再生することが可能となる。

以上のように、本実施の形態の情報再生装置800では、第5の実施の形態の情報再生装置の特徴に加えて、光ディスクドライブ509とSCSI制御回路内蔵AVデコードカード801が直接コマンドおよびデータの送受信を行うために、相互認証方式や鍵情報を不当に解読されること、および、ソフトウェアによって不当なコピー動作が実行されることに対するセキュリティが向上する。

なお、再生する情報記録媒体を本発明に係る情報記録媒体の第4の実施の形態を用いて説明したが、本発明に係る情報記録媒体の第3の実施の形態においても全く同様に処理することが可能であり、説明中の暗号化タイトル鍵をシードキーとし、暗号化ディスク鍵をスクランブル情報セクタの変換テーブル情報に置き換えれば良い。

なお、本実施の形態では、光ディスクドライブ509が接続されるバスをSCSIバスであるとしたが、定められたプロトコルに従って再生データが転送できればこれに限らず、ATAPI、IEEE1394等のインタフェースでも良い。

(第7の実施形態)

次に、本発明に係る情報再生装置1000を説明する。

図19は、本発明に係る情報再生装置1000の構成を示すブロック図である。情報再生装置1000は光ディスクプレーヤである。情報再生装置1000の構成要素は、プログラムROM1001を除いて、図14の情報再生装置の構成要素または図17の情報再生装置の構成要素と同一である。従って、同一の構成要素には同一の参照番号を付し、その説明を省略する。また、ここでは本発明の情

不可能であり、相互認証処理が不要であることによる。したがって、本実施の形態の構成には、相互認証処理を実行する構成要素が存在しなくとも、著作権保護が可能となる。また、光ディスクプレーヤ 1000 は再生時に用途識別情報の判定を行うために、再生が禁止されている用途のデータを再生することを防止できる。

以下に、本発明に係る情報再生装置の第 5 の実施の形態および第 6 の実施の形態において使用される、デコーダ認証回路 601、ドライブ認証回路 701、デスクランブル回路 705 の更に詳細な構成および動作を説明する。ただし、以下で述べる構成については、本発明の情報再生装置の第 5 の実施の形態、第 6 の実施の形態および第 7 の実施の形態に共通の構成となっている。

まず、デスクランブル回路 705 の構成と動作についてを図面を参照して説明する。ただし、デスクランブル回路 705 は、スクランブル方式と深く関係するために、本発明の情報記録媒体の第 3 の実施の形態を再生する場合と第 4 の実施の形態を再生する場合とで異なる構成となる。従って以下では、本発明の情報記録媒体の第 3 の実施の形態を再生するためのデスクランブル回路を図 20 および図 21 を用いて、本発明の情報記録媒体の第 4 の実施の形態を再生するためのデスクランブル回路を図 22 および図 23 を用いて、それぞれ独立に説明する。

図 20 は、本発明の情報記録媒体の第 3 の実施の形態を再生するためのデスクランブル回路 1106 の構成を示すブロック図である。以下、各構成要素について説明する。1100 は制御バス 704 との通信を行うための I/O 制御回路を、1101 は入力されるデータの内容に応じて出力先のブロックを切り替えるセレクタを、1102 は再生フィルの用途識別情報を参照して再生許可であるか否かを判定する用途識別回路を、1103 はシードキーから乱数発生回路 1104 のためのプリセットデータを生成する変換テーブルを格納しておくための変換テーブル記憶回路を、1104 は前記変換テーブル記憶回路 1103 から出力されるプリセットデータをもとに乱数を発生させる乱数発生回路を、1105 は乱数発

生回路 1104 で発生された乱数とセクタ 1101 から入力されるスクランブルデータとの論理演算を行うことによりデスクランブル処理を行うメインデータデスクランブル回路を、それぞれ示している。

次に、デスクランブル回路 1106 の動作を説明する。

5 まず、相互認証処理が正常に終了した後にリードイン領域に記録されたスクランブル情報セクタを読み出す場合、I/O制御回路 1100 を介してセクタ 1101 にスクランブル情報セクタ読み出し設定がなされ、セクタ 1101 は出力先を変換テーブル記憶回路 1103 に設定する。入力された読み出しデータはセクタ 1101 を介して変換テーブル記憶回路 1103 に入力され、乱数発生
10 の初期値となるプリセットデータを決定する変換テーブルとして格納される。

一方、スクランブルファイルの再生時には、データの再生に先立って相互認証処理が行われ、相互認証処理の正常終了後に受け取ったセクタヘッダ領域中の用途識別情報が用途識別回路 1102 に、シードキーが変換テーブル記憶回路 1103 にそれぞれ入力される。用途識別回路 1102 では、内部に再生を許可された用途識別情報に関する情報を有しており、入力された用途識別情報と比較することにより、再生を許可されているか否かを識別し、I/O制御回路 1100 と
15 メインデータデスクランブル回路 1105 に報告する。一方、シードキーを受領した変換テーブル記憶回路 1103 は、受け取ったシードキーをもとに、シードキーに対応したプリセットデータを乱数発生回路 1104 に出力する。乱数発生
20 回路 1104 は受け取ったプリセットデータをもとに乱数系列を発生してメインデータデスクランブル回路 1105 に出力する。さて、セクタヘッダ領域に引き続いてスクランブルセクタのメインデータが入力される際には、セクタ 1101 の出力先はメインデータデスクランブル回路 1105 に切り替えられる。その後、メインデータデスクランブル回路 1105 は、セクタ 1101 から入力されるメインデータと、乱数発生回路 1104 から入力される乱数系列の論理演算
25 を行うことによってデスクランブル処理を実行し、デスクランブル後のデータを

オーディオビデオデコード回路 706 に出力する。

以上の動作についてのより詳細な説明を図 21 を用いて以下に示す。

図 21 はデスクランブル回路 1106 において、本発明の第 3 の実施の形態の情報記録媒体を再生する場合のデスクランブル処理内容を説明するためのフローチャートである。以下にその各処理ステップについて説明する。

(S1200) セレクタ 1101 の出力先を変換テーブル記憶回路 1103 に切り替えて、情報記録媒体のリードイン領域のスクランブル情報セクタから読み出された変換テーブルを変換テーブル記憶回路 1103 に格納。

(S1201) セレクタ 1101 の出力先を I/O 制御回路 1100 に切り替え、スクランブルファイルの再生に先立って受領したセクタヘッダ中のスクランブルフラグをマイクロコントローラ 702 に返送する。マイクロコントローラ 702 はスクランブルフラグが 1 であるか否かを判定し、I/O 制御回路 1100 に判定結果を返送する。スクランブルフラグが 1 であると判定されれば (S1202) へ、0 であると判定されればメインデータデスクランブル回路 1105 の機能を停止状態として (S1206) へ分岐。

(S1202) セレクタ 1101 の出力先を用途識別回路 1102 に切り替え、スクランブルファイルの再生に先立って受領したセクタヘッダ中の用途識別情報を転送。用途識別回路 1102 は受け取った用途識別情報と内部に保持している再生許可情報とを比較して、再生が許可されたファイルであるか否かを判定。再生禁止と判定すれば (S1203) へ、再生許可されていると判定すれば (S1204) に分岐。

(S1203) 上記処理ステップ (S1202) で再生禁止のファイルであると判定した場合には、本ステップで I/O 制御回路 1100 を介してマイクロコントローラ 702 にエラーを報告して処理を終了。

(S1204) 変換テーブル記憶回路 1103 は再生するスクランブルファイルのセクタヘッダから読み出したシードキーを入力され、シードキーと変換テ

ープルとからプリセットデータを生成し、乱数発生回路 1104 に出力。

(S1205) セレクタ 1101 の出力先をメインデータデスクランブル回路 1105 に切り替え、メインデータデスクランブル回路 1105 に入力されるスクランブルファイルのメインデータを転送。一方、乱数発生回路 1104 は変換テーブル記憶回路 1103 から入力されたプリセットデータをもとに乱数系列を発生し、メインデータデスクランブル回路 1105 に出力。メインデータデスクランブル回路 1105 では、入力されたメインデータと乱数系列との論理演算を行うことによってデスクランブル処理を実行。

(S1206) メインデータデスクランブル回路 1105 は、デスクランブル実行時にはデスクランブル後データを、デスクランブル機能を停止状態なら、セレクタ 1101 から入力されたデータをそのままオーディオ／ビデオデコーダ回路 706 に出力。

以上のように、デスクランブル回路 1106 は、用途識別回路を有することにより、再生を禁止された用途識別情報を有するファイルと再生を許可された用途識別情報を有するファイルとを選択的に再生することが可能である。

また、内部にスクランブル識別フラグを分離するセレクタを有するために、スクランブルフラグのみ分離し、デスクランブルを行う／行わないの判定を行うことを可能とする。

また、ディスク単位にプリセットデータに変換するための変換テーブルを決定でき、ファイル単位にシードキーを決定できるため、前記の 2 つのデータが共になくとも再生できないようなセキュリティの高いスクランブル方式をもつ情報記録媒体の再生が可能である。

図 22 は、本発明の情報記録媒体の第 4 の実施の形態を再生するためのデスクランブル回路 1308 の構成を示すブロック図である。以下、各構成要素を説明する。1300 は制御バス 704 との通信を行うための I/O 制御回路を、1301 は入力されるデータの内容に応じて出力先のブロックを切り替えるセレクタ

を、1302は暗号化ディスク鍵が入力された場合に暗号化ディスク鍵の復号処理を行うディスク鍵復号化回路を、1303は暗号化ディスク鍵を復号時に使用するマスター鍵をハードウェア的に格納するマスター鍵格納部を、1304はディスク鍵復号回路1302で復号されたディスク鍵を受け取り、セクタヘッダ中の暗号化部の復号を行うセクタヘッダ復号回路を、1305は媒体識別情報およびセクタヘッダ復号回路1304で復号されたオリジナルCGMSデータと、セクタから入力されたメディアCGMSデータの整合性の確認を行うCGMS検査回路を、1306はセクタヘッダ復号回路1304で復号された用途識別情報を受け取って再生が許可されているか否かを判定する用途識別回路を、1307はセクタヘッダ復号回路1304から入力されるタイトル鍵をもとにセクタ1301から入力されるメインデータをデスクランブルするメインデータデスクランブル回路を、それぞれ示している。

以下に、デスクランブル回路1308の動作を説明する。

まず、相互認証処理が正常に終了した後にリードイン領域に記録されたスクランブル情報セクタを読み出す場合、I/O制御回路1300を介してセクタ1301の出力先がディスク鍵復号回路1302に設定され、入力された読み出しデータはセクタ1301を介してディスク鍵復号化回路1302に入力される。ディスク鍵復号化回路1302では、マスター鍵格納部1303から入力されるマスター鍵をもとにディスク鍵を復号し、ディスク鍵復号化回路1302の内部に格納される。

一方、スクランブルファイルの再生時には、データの再生に先立って相互認証処理が行われ、相互認証処理の正常に終了すれば、再生するスクランブルファイルのセクタヘッダがセクタ1301に入力される。セクタ1301はセクタヘッダの内容毎に出力先を選定し、スクランブルフラグをI/O制御回路1300を介してマイクロコントローラ702に、メディアCGMSデータをCGMS検査回路1306に、暗号化オリジナルCGMSデータおよび暗号化用途識別情

報および暗号化タイトル鍵（以下では、これらをあわせて暗号化セクタヘッドと称す）をセクタヘッド復号回路 1304 に出力する。セクタヘッド復号回路 1304 はディスク鍵復号回路 1302 からディスク鍵を受領し、ディスク鍵をもとに暗号化セクタヘッドを復号し、オリジナル CGMS データを CGMS 検査回路 1305 に、用途識別情報を用途識別回路 1306 に、タイトル鍵をメインデータデスクランブル回路 1307 に、それぞれ出力する。CGMS 検査回路 1305 はセクタ 1301 から入力されるメディア CGMS データとセクタヘッド復号回路 1304 から入力されるオリジナル CGMS とを受け取り、再生の許可された値か否かを判定する。この時、CGMS 検査回路 1305 の判定の基準を（表 2）に示す。（ただし、メディア CGMS データとオリジナル CGMS データが示す意味については、本発明の第 4 の実施の形態の情報記録媒体の説明に準ずるものとする。）

表 2

媒体識別情報	メディアCGMS データ	オリジナルCGMS データ	CGMS 判定情報
1 (再生専用型媒体)	00	00	1
		01/10/11	0
	01	00/01/10/11	0
		00/01/11	0
	10	10	1
		00/01/10	0
	11	11	1
0 (書換型媒体)	00	00	1
		01/10/11	0
	01/10	00/01/10/11	0
	11	10	1
		00/01/11	0

(表2)において、CGMS判定情報が1を示す場合には、再生可能であるとしてメインデータデスクランブル回路1307とマイクロコントローラ702に報告する。一方、CGMS判定情報が0の場合には不正コピー等の行われた可能性があることを意味する妥当でない値であるとして、メインデータデスクランブル回路1307およびマイクロコントローラ702にエラーを報告する。例えば、

(表2)において、媒体識別情報が書換型媒体を示す0であって、メディアCGMSデータがコピー禁止を示す11であって、オリジナルCGMSデータが1回コピーのみ許可を示す10である場合には、1回のみコピー許可のファイルが書換型媒体に既に1回コピーをされてメディアCGMSデータのみが11となっており、コピー禁止に変更されたと考えられるため、出力は再生許可を意味する1となっている。一方、仮に上記のような1回のみコピー許可であるファイルが不正なコピーをされた場合には、メディアCGMSデータとオリジナルCGMSデータが共に1回のみコピー許可を意味する10となるために、その場合のCGMS判定情報は再生禁止を意味する0となっている。一方、用途識別回路1306は、再生の許可されている用途識別情報を内部に有しており、その情報とセクタヘッダ復号回路1304から入力される用途識別情報を比較して、スクランブルファイルが再生を許可された用途であるか否かを判定する。再生の許可されていない用途識別情報であった場合には、マイクロコントローラ702およびメインデータデスクランブル回路1307にエラーを報告する。スクランブルファイルのデータを再生する場合には、セクタ1301の出力先はメインデータデスクランブル回路1307に切り替えられ、入力される読み出しデータはメインデータデスクランブル回路1307に転送される。メインデータデスクランブル回路1307は、セクタヘッダ復号回路1304からタイトル鍵を受け取り、受け取ったタイトル鍵をもとにスクランブルデータのデスクランブル処理を施してオーディオ／ビデオデコード回路706に出力する。

以上のように、デスクランブル回路1308は暗号化ディスク鍵、暗号化タイ

トル鍵の復号を行い、タイトル鍵が再生の許可されたものであれば、メインデータのデスクランブル処理を行って、スクランブル後のデジタルAVデータをオーディオ／ビデオデコーダ回路706に出力する。

次に、デスクランブル回路1308におけるスクランブルファイルの再生処理の動作について、図23のフローチャートを用いて説明する。以下に各ステップの処理内容を示す。

(S1400) 読み出しデータにリードイン領域の暗号化ディスク鍵情報が入力される場合に、セクタ1301の出力先はディスク鍵復号回路1302に設定され、暗号化ディスク鍵をディスク鍵復号回路1302に転送。ディスク鍵復号回路1302はマスター鍵格納部1303からマスター鍵を受け取り暗号化ディスク鍵を復号し、復号されたディスク鍵をセクタヘッダ復号回路1304に出力。

(S1401) 再生に先立って読み出されたスクランブルファイルのセクタヘッダから、セクタ1301はスクランブルフラグを分離し、I/O制御回路1300を介してマイクロコントローラ702に転送。マイクロコントローラ702はスクランブルフラグが1であるか否かを判定。判定結果が、1であれば(S1402)へ、1でなければ(S1407)へ分岐。

(S1402) 再生に先立って読み出されたスクランブルファイルのセクタヘッダから、セクタ1301は暗号化セクタヘッダを分離し、セクタヘッダ復号回路1304へ転送。セクタヘッダ復号回路1304は、あらかじめディスク鍵復号回路1302から受け取ったディスク鍵をもとに、受け取った暗号化セクタヘッダを復号し、内容毎に分離し、オリジナルCGMSデータをCGMS検査回路1305に、用途別識別情報を用用途識別回路1306に、タイトル鍵をメインデータデスクランブル回路1307に、それぞれ出力。

(S1403) CGMS検査回路1305は、マイクロコントローラ702から受け取った媒体識別情報と、セクタ1301から受け取ったメディアCG

MSデータと、セクタヘッダ復号回路1304から受け取ったオリジナルCGMSデータから、(表2)に応じたCGMS判定情報を出力。ただし、(表2)において、CGMS判定情報が1の場合には、I/O制御回路1300とメインデータデスクランブル回路1307に正常なCGMS制御情報であることを報告。

5 (S1404) CGMS判定結果が0であった場合にはCGMS検査回路1305が、用途識別情報が再生を禁止された用途であった場合には用途識別回路1306が、I/O制御回路1300およびメインデータデスクランブル回路1307にエラーを報告し、再生処理を終了する。

10 (S1405) 用途識別回路1306は、セクタヘッダ復号回路1304から受け取った用途識別情報を判定し、再生を許可された場合にはI/O制御回路1300およびメインデータデスクランブル回路1307に再生を許可されたファイルであることを報告。

15 (S1406) セレクタ1301は、読み出しデータとしてスクランブルファイルのメインデータを受け取ると、出力先をメインデータデスクランブル回路1307に設定し、メインデータを転送。メインデータデスクランブル回路1307はセクタヘッダ復号回路1304から受け取ったタイトル鍵をもとに、入力されたメインデータのデスクランブル処理を実行。

20 (S1407) メインデータデスクランブル回路1307は、デスクランブル処理を実行した場合にはデスクランブル後のメインデータを、デスクランブル処理を実行しなかった場合にはセレクタ1301から入力されたデータをそのままオーディオ/ビデオデコーダ回路706に出力。

以上のように、デスクランブル回路1308は、用途識別回路を有することにより、再生を禁止された用途識別情報を有するファイルと再生を許可されたように識別情報を有するファイルとを選択的に再生することが可能である。

25 また、内部にスクランブル識別フラグを分離するセレクタを有するために、スクランブルフラグのみ分離し、デスクランブルを行う/行わないの判定を行うこ

とを可能とする。

また、本発明の情報記録媒体の第4の実施の形態のような階層的に暗号／スクランブル化されたセキュリティの高いディスクであっても、ディスク鍵復号回路、セクタヘッダ復号回路、メインデータデスクランブル回路が連携して動作することにより、デスクランブルを行わないときと同様に処理することが可能となる。

また、CGMS検査回路1305を有することによって、不正にコピーされたデータを検出することが可能となり、不正コピーデータの再生を防止することが可能となる。さらに、コピーが何度繰り返されたデータであるかという、コピーの世代を管理することが可能となり、ある定められた回数だけのコピー動作を許可するようなソフトウェアが記録された情報記録媒体の著作権を保護する機構を有する。

図24は、光ディスクドライブ509内のデコーダ認証回路601の詳細な構成を示すブロック図である。以下、各構成要素について説明する。1500はマイクロコントローラ602との通信を行うための入出力制御を行うI/O制御回路を、1501はI/O制御回路1500から入力される時変鍵をもとに乱数を発生する乱数発生回路を、1502は関数を決定するための第1の入力(図24ではkと表記)によって関数fkを決定し、その引数となる第2の入力(図24ではR1と表記)から関数値fk(R1)を計算して出力する関数fk(R1)生成回路を、同様に1503はkとR2から関数gk(R2)を計算して出力すると共にI/O制御回路1500から入力されるデコーダ応答データとの比較を行う関数gk(R2)生成・比較回路を、1504は関数gk(R2)生成・比較回路1503と関数fk(R1)生成回路1502から出力される2つの関数値をもとにバス鍵を生成するバス鍵生成回路を、1505はバス鍵生成回路1504から出力されるバス鍵に従ってデータ再生回路606から出力されるデータを暗号化するバス暗号化回路を、それぞれ示している。

以下、デコーダ認証回路601の動作を説明する。

光ディスクドライブ 509 のリセット時やディスク交換時に、マイクロコントローラ 602 はディスクのリードイン領域のスクランブル情報セクタのセクタヘッダ領域から読み出した相互認証鍵 k を I/O 制御回路 1500 を介して関数 f_k (R1) 生成回路 1502 および関数 g_k (R2) 生成・比較回路 1503 にあらかじめ設定する。

関数 f_k (R1) 生成回路 1502 は相互認証鍵 k を内部的に保持しており、その後の相互認証処理時に乱数値 R_1 が入力された場合に関数値 f_k (R1) を計算し、バス鍵生成回路 1504 および I/O 制御回路 1500 に出力する。

バス鍵生成回路 1504 は入力された関数値 f_k (R1) を内部的に格納する。引き続き、マイクロコントローラ 602 から I/O 制御回路 1500 を介して乱数発生のための時変鍵が入力された場合に乱数発生回路 1501 は、時変鍵をもとに乱数 R_2 を発生して I/O 制御回路 1500 に返送すると共に、関数 g_k (R2) 生成・比較回路 1503 に出力する。

乱数 R_2 を受け取った関数 g_k (R2) 生成・比較回路 1503 は、前もって保持していた相互認証鍵 k および乱数値 R_2 から関数値 g_k (R2) を計算して内部的に保持する。更に関数 g_k (R2) 生成・比較回路 1503 は、I/O 制御回路 1500 からデコード応答データを受け取り、内部で計算した関数値 g_k (R2) と比較を行う。比較の結果、 g_k (R2) の値とデコード応答データが一致しなかった場合には、I/O 制御回路 1500 を介してマイクロコントローラ 602 に相互認証処理でエラーが発生したことを報告する。相互認証処理に失敗した場合には、相互認証処理に続く暗号化ディスク鍵および暗号化タイトル鍵の転送等の処理は中止される。

一方、 g_k (R2) とデコード応答データの 2 つの値が一致した場合は相互認証処理が正常に終了したと判定され、関数値 g_k (R2) がバス鍵生成回路 1504 に出力される。この時、バス鍵生成回路 1504 は、関数値 f_k (R1) および g_k (R2) が正常に入力された場合にのみ、二つの関数値 f_k (R1) および g_k (R2) をもとにバス鍵を生成し、バス暗号化回路 1505 に出力する。

バス暗号化回路 1505 は、I/O 制御回路 1500 を介してマイクロコント
ローラ 602 からモードを切り替えるための制御信号（以下、モード制御信号と
称す）を受け取り、モードがディスク鍵再生モードであるか、またはタイトル鍵
再生モードであれば、データ再生回路 606 から入力される暗号化ディスク鍵又
5 は暗号化タイトル鍵に対して、あらかじめ入力されたバス鍵をもとに所定の暗号
化を施し、SCSI 制御回路 600 に出力する。

一方、暗号化タイトル鍵の送出後に、実際のファイルデータを送出する場合に
は、モード制御信号はデータ再生モードに切り替えられ、バス暗号化回路 150
5 はバス暗号化は行わずにデータ再生回路 606 から出力されるデータをそのま
10 ま SCSI 制御回路 600 に出力する。

以上のようにデコード認証回路 601 では、相互認証処理において相互認証鍵
で決定される関数値計算を行って、デコードから送られる関数値と一致した場合
のみ相互認証処理を正常に終了する。更に、再生動作においても、暗号化ディス
ク鍵、暗号化タイトル鍵の転送時には、相互認証処理において生成したバス鍵を
15 用いて更に暗号化した鍵情報を送出する処理を行う。

次に、AV デコーダカード 507 および SCSI 制御回路内蔵 AV デコーダカ
ード 801 上のドライブ認証回路 701 の構成および動作について図面を参照し
て説明する。

図 25 は、ドライブ認証回路 701 の構成を示すブロック図である。以下、各
構成要素について説明する。1600 はマイクロコントローラ 702 との制御信
20 号の送受信を行うための I/O 制御回路を、1601 は I/O 制御回路 1600
から時変鍵を受信して乱数 R1 を発生し、I/O 制御回路 1600 に返送すると
共に関数 $fk(R1)$ 生成・比較回路 1603 に出力する乱数発生回路を、1602 は
関数 $fk(R1)$ 生成・比較回路 1603 から入力される定数 k と I/O 制御回路 16
25 00 から入力される乱数 R2 をもとに関数 $gk(R2)$ を計算する関数 $gk(R2)$ 生成回路
を、1603 は乱数発生回路 1601 から入力される乱数 R1 をもとに k が 1 か

ら n までについて関数 $f_k(R1)$ の値を計算して、I/O 制御回路 1600 から入力されるドライブ応答データと一致するか比較する関数 $f_k(R1)$ 生成・比較回路を、1604 は関数 $g_k(R2)$ 生成回路 1602 から出力される関数値と関数 $f_k(R1)$ 生成・比較回路 1603 から出力される関数値からバス鍵を生成するバス鍵生成回路を、1605 はバス鍵生成回路 1604 から出力されるバス鍵によってデータの復号を行うバス復号化回路を、それぞれ示す。

次に、ドライブ認証回路 701 の動作を説明する。

まず、相互認証処理の開始時にドライブ認証回路 701 は、I/O 制御回路 1600 を介してマイクロコントローラ 702 から乱数発生のための時変鍵を受け取り、乱数発生回路 1601 によって乱数が発生される。

乱数発生回路 1601 は発生した乱数 $R1$ を関数 $f_k(R1)$ 生成・比較回路 1603 およびマイクロコントローラ 702 に出力する。その後、関数 $f_k(R1)$ 生成・比較回路 1603 は、マイクロコントローラ 702 からドライブ応答データを受け取り、内部に保持している乱数値 $R1$ を引数として関数 $f1(R1)$, $f2(R1)$, $f3(R1)$... を計算し、ドライブ応答データと $f_k(R1)$ が一致するような k を求める。この時、保持している全ての関数計算を行ってもドライブ応答データと一致する k を求めることができなかった場合に関数 $f_k(R1)$ 生成・比較回路 1603 は、認証結果としてエラーを I/O 制御回路 1600 を介してマイクロコントローラ 702 に返送する。

一方、ドライブ応答データと $f_k(R1)$ が一致するような k が発見された場合は、認証結果として正常終了をマイクロコントローラ 702 に返送し、 k を関数 $g_k(R2)$ 生成回路 1602 に出力し、関数値 $f_k(R1)$ をバス鍵生成回路 1604 に出力する。正常に k の値を発見できた場合にドライブ認証回路 701 は、引き続いて乱数 $R2$ をマイクロコントローラ 702 から受け取り関数 $g_k(R2)$ 生成回路 1602 に入力する。関数 $g_k(R2)$ 生成回路 1602 は、あらかじめ関数 $f_k(R1)$ 生成・比較回路 1603 から受け取った値 k と、入力された乱数 $R2$ から関数 $g_k(R1)$ を計算

し、計算した関数値をマイクロコントローラ 702 およびバス鍵生成回路 1604 に出力する。

バス鍵生成回路 1604 は前もって受け取った関数値 $fk(R1)$ と、 $gk(R2)$ の 2 つの関数値をもとにバス鍵を生成し、バス復号回路 1605 に出力する。一方、マイクロコントローラ 702 に送出した関数値 $gk(R2)$ が光ディスクドライブ 509 で正常に認証された場合には、マイクロコントローラ 702 がモード制御信号を切り替えて、バス復号化回路 1605 のモードをディスク鍵再生モードまたはタイトル鍵再生モードに切り替え、復号処理機能使用状態とする。

この時、SCSI 制御回路 900 又はシステムインタフェース回路 700 から入力されるデータ（暗号化ディスク鍵又は暗号化タイトル鍵）はバス復号化回路 1605 においてあらかじめ保持されているバス鍵によって復号される。ただし、バス復号化回路 1605 によって復号されるのはバス鍵によるバス暗号のみであり、マスター鍵によって暗号化された暗号化ディスク鍵、ディスク鍵によって暗号化された暗号化タイトル鍵は暗号化されたままデスクランブル回路 705 に出力される。

またその後に、スクランブルファイルの再生データが SCSI 制御回路 900 又はシステムインタフェース回路 700 から入力される際にバス復号化回路 1605 は、マイクロコントローラ 702 からのモード制御信号によってデータ再生モードに切り替えられ、バス鍵による復号処理を行わずにデスクランブル回路 705 にデータをそのまま転送する。

以上のようにドライブ認証回路 701 では、内部で発生した乱数から複数の関数値を計算し、そのうちのいずれか一つとドライブ応答データが一致することでドライブを認証し、逆に乱数を受領して内部の関数値を計算して返送することで光ディスクドライブ 509 から認証されるという、相互認証処理を実行する。

また、再生動作においても、暗号化ディスク鍵、暗号化タイトル鍵の受信時には、相互認証処理において生成したバス鍵を用いて復号処理を行う。

次に、本発明の情報再生装置の第5の実施の形態および第6の実施の形態において実行される相互認証処理のフローチャートについて図面を参照して説明する。

図26は、光ディスクドライブ509とAVデコーダカード507又はSCSI制御回路内蔵AVデコーダカード801間の相互認証処理を説明するためのフローチャートである。

相互認証処理は、装置のリセット時やディスク交換時、および読み出そうとしたファイルがスクランブルファイルであることがファイル管理情報から確認された時等に、適宜実行される。以下、各処理ステップについて説明する。ただし、AVデコーダカード507又はSCSI制御回路内蔵AVデコーダカード801を、以下では単にAVデコーダと称することとする。また、以下では、SCSIプロトコル上でのコマンドを、デバイスコマンドと称する。

(S1700) AVデコーダは、タイマー等を用いて発生させた時間と共に変化する時変鍵をもとに乱数R1を生成。

(S1701) 光ディスクドライブはデバイスコマンド"Send R1"によって、AVデコーダが生成した乱数R1を受け取る。この時光ディスクドライブは、装着されているディスクの相互認証鍵kを未だ格納していなければ、リードイン領域のスクランブル情報セクタのセクタヘッダ領域から相互認証鍵の読み出しを実行。

(S1702) 光ディスクドライブがステップ(S1701)の処理中に何らかのエラーを検出してエラー報告が行われた場合には、ステップ(S1713)に分岐、正常に終了すればステップ(S1703)に分岐。

(S1703) 光ディスクドライブは、デバイスコマンド"Report fk(R1)"を受領し、あらかじめ受け取った乱数値R1とディスクから読み出した相互認証鍵kの値をもとに、関数fk(R1)の値を計算し、計算結果をAVデコーダに返送する。以上の処理において何らかのエラーが生じた場合に光ディスクドライブは、コマンドの処理結果としてエラーを報告。

(S 1 7 0 4) デバイスコマンド"Report fk(R1)"処理中に何らかのエラーが発生し、コマンド処理結果がエラーとなっていればステップ(S 1 7 1 3)に分岐、処理結果が正常終了であればステップ(S 1 7 0 5)に分岐。

5 (S 1 7 0 5) AVデコーダは、内部に保持する関数値生成回路を使用して、1からn(nは正の整数)までのi(iは正の整数)について関数値fi(R1)を計算し、計算したfi(R1)の値と、(S 1 7 0 3)において光ディスクドライブから返送されたfk(R1)の値を比較する。AVデコーダはfi(R1)=fk(R1)となるようなiの値を検出すれば、その値を内部的に保持。

10 (S 1 7 0 6) 前記処理ステップ(S 1 7 0 5)において、AVデコーダがfi(R1)=fk(R1)となるようなiを検出できなかった場合にはステップ(S 1 7 1 3)に分岐、検出した場合にはステップ(S 1 7 0 7)に分岐。

15 (S 1 7 0 7) 光ディスクドライブはデバイスコマンド"Report R2"コマンドを受け取り、内部の乱数発生機構で時間と共に変化する時変鍵をもとに乱数を生じ、AVデコーダに転送する。なお、本ステップで光ディスクドライブが何らかのエラーを検出した場合には、エラーを報告。

(S 1 7 0 8) 前記ステップ(S 1 7 0 7)において、"Report R2"コマンド実行過程で、何らかのエラーが発生した場合にはステップ(S 1 7 1 3)に分岐、正常に終了した場合にはステップ(S 1 7 0 9)に分岐。

20 (S 1 7 0 9) (S 1 7 0 8)において"Report R2"コマンドによって光ディスクドライブが発生した乱数R2を受け取ったAVデコーダは、内部の関数計算回路を使用して、既にステップ(S 1 7 0 5)において格納した定数k(=i)と、ステップ(S 1 7 0 7)において光ディスクドライブから受信した乱数値R2をもとに、関数値gk(R2)を計算。

25 (S 1 7 1 0) 関数値gk(R2)を計算したAVデコーダは、デバイスコマンド"Send gk(R2)"を実行して、ステップ(S 1 7 0 9)において計算した関数値を光ディスクドライブに転送する。関数値gk(R2)を受け取った光ディスクドライブは、

内部に有する関数計算回路において、相互認証鍵 k と乱数値 R_2 を用いて $gk(R_2)$ を計算する。その後光ディスクドライブは、AVデコーダから受け取った関数値 $gk(R_2)$ と、内部の計算回路によって計算した $gk(R_2)$ とを比較し、一致した場合には正常終了を処理結果として報告する。一方、コマンド処理中に何らかのエラーが生じた場合や、受信した関数値と内部で計算した関数値とが一致しなかった場合には、コマンド処理結果としてエラーを報告。

(S1711) 前記ステップ (S1710) において、コマンド処理結果がエラーであればステップ (S1713) に分岐、正常終了であれば (S1712) に分岐。

(S1712) AVデコーダは、上記の相互認証処理中において取得した2つの関数値 $fk(R_1)$ および $gk(R_2)$ をもとに、内部に保持するバス鍵生成回路を用いてバス鍵 BK を生成する。同様に、光ディスクドライブも、上記相互認証処理中に取得した2つの関数値から内部に保持するバス鍵生成回路を用いてバス鍵 BK を生成。(ここで、光ディスクドライブとAVデコーダが相互認証処理中で、生成されるバス鍵 BK は同一となる)。

(S1713) デバイスコマンド実行中にエラーが生じた場合、本ステップにおいてエラー報告と共に相互認証処理を中止。

以上のように相互認証処理を行うことによって、不正コピーを行う機器へのデータ転送でないことを光ディスクドライブが確認した後に鍵情報を転送することができるために、デスクランブルを行うための鍵情報を隠す効果がある。従って、スクランブル方式の不正な解読を防止する効果がある。

また、AVデコーダがデータを受け取る機器が不正コピーしたデータを転送する機器でないことを確認した後に鍵情報の復号化およびデータのデスクランブルを行うことができるために、不正コピーされたデータ再生を防止する効果がある。

また、相互認証処理の度に異なるバス鍵を生成するために、鍵情報を不正に読み出されることを防止すると共に、暗号化/スクランブル方式の不正な解読を防

止する効果がある。

また、相互認証において光ディスクドライブがAVデコーダを認証する場合と、AVデコーダが光ディスクドライブを認証する場合とで、異なる関数を用いているために、相互認証動作を不正に実行することを目的として相互認証動作の方式を解読しようとする行為に対するセキュリティが高い。

また、相互認証処理において、光ディスクドライブ、AVデコーダの各々が生成した時変鍵を用いているために、相互認証処理を実行する度に異なる乱数値が発生され、異なる関数値が転送され、異なるバス鍵が生成されるため、相互認証動作を不正に実行することを目的として相互認証動作の方式を解読しようとする行為に対するセキュリティが高い。

また、情報記録媒体上に記録された相互認証鍵を相互認証処理に用いることにより、相互認証動作を不正に実行することを目的として相互認証動作の方式を解読しようとする行為に対するセキュリティが高い。

なお、上記説明では、情報記録媒体として本発明の情報記録媒体の第4の実施の形態を例に説明したが、本発明の情報記録媒体の第3の実施の形態についても同様に処理することが可能である。

産業上の利用の可能性

本発明の情報記録媒体は、リードイン領域とデータ記録領域とを有している。リードイン領域に記録された鍵情報に基づいて、データ記録領域に記録されたスクランブルされたデータがデスクランブルされる。このように、リードイン領域に鍵情報を記録することにより、セキュリティが向上する。情報記録媒体のドライブ装置は、リードイン領域を直接的にアクセスすることができるのに対し、ドライブ装置以外の装置（例えば、パーソナルコンピュータ）は、リードイン領域を直接的にアクセスすることができないからである。さらに、リードイン領域に鍵情報を記録することにより、鍵情報を読み出すための専用の読み出し手段を設

ける必要がない。

- 本発明の他の情報記録媒体は、リードイン領域とデータ記録領域とを有している。リードイン領域に記録された第1の鍵情報とデータ記録領域に記録された第2の鍵情報とに基づいて、スクランブルされたデータがデスクランブルされる。
- 5 このように、デスクランブルのための鍵情報が二重化されているため、セキュリティが向上する。

- 本発明の情報再生装置によれば、スクランブルされたデータがデコード装置に送信される前に、相互認証処理が行われる。相互認証処理により相手方が正規であることが相互に確認される。これにより、セキュリティが向上する。
- 10 本発明の情報再生装置によれば、読み出し装置とデコード装置との間で相互認証処理が行われる。相互認証処理が正常に終了すると、読み出し装置とデコード装置とに共通なバス鍵情報が生成され、バス鍵情報によって暗号化された鍵情報が読み出し装置からデコード装置に送信される。このように、相互認証処理を行った後、さらに共通のバス鍵を使用することにより、相手方が正規であることが
- 15 相互に確認される。これにより、セキュリティが向上する。

請求の範囲

1. リードイン領域とデータ記録領域とを有する情報記録媒体であって、
該リードイン領域には、鍵情報が記録され、
5 該データ記録領域には、スクランブルされたデータが記録され、
該スクランブルされたデータは、該鍵情報に基づいてデスクランブルされる、
情報記録媒体。
2. リードイン領域とデータ記録領域とを有する情報記録媒体であって、
10 該リードイン領域には、第1の鍵情報が記録され、
該データ記録領域には、第2の鍵情報と、スクランブルされたデータとが記録
され、
該スクランブルされたデータは、該第1の鍵情報に基づいて該第2の鍵情報
を変換することによって得られる情報に基づいてデスクランブルされる、情報記録
15 媒体。
3. 前記データ記録領域は、複数のセクタに分割されており、該複数のセクタの
それぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクラン
ブルされたデータを記録するメインデータ領域とを含んでおり、前記第2の鍵情
20 報は、該セクタヘッダ領域に記録されている、請求項2に記載の情報記録媒体。
4. 前記第2の鍵情報は、前記第1の鍵情報によって暗号化されており、前記情
報は、該暗号化された第2の鍵情報を復号化することによって得られる、請求項
25 2に記載の情報記録媒体。
5. 前記第1の鍵情報は、マスター鍵情報によって暗号化されている、請求項4

に記載の情報記録媒体。

5 6. 前記リードイン領域には、複数の第1の鍵情報が記録されており、該複数の第1の鍵情報は、複数の異なるマスター鍵情報によってそれぞれ暗号化されている、請求項4に記載の情報記録媒体。

10 7. 前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録されている、請求項2に記載の情報記録媒体。

15 8. 前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記スクランブルフラグは、該セクタヘッダ領域に記録されている、請求項7に記載の情報記録媒体。

20 9. 前記データ記録領域は、複数のファイルを記録する領域と、該複数のファイルを管理する情報を記録するファイル管理領域とを含んでおり、前記スクランブルフラグは、該ファイル管理領域に記録されている、請求項7に記載の情報記録媒体。

25 10. 前記リードイン領域には、前記スクランブルされたデータを読み出す読み出し装置と該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置との間で相互認証を行うための相互認証鍵情報がさらに記録されている、請求項2に記載の情報記録媒体。

- 1 1. 前記情報は、乱数系列を生成するための初期値であり、前記スクランブルされたデータは、該乱数系列に対して論理演算を行うことによりデスクランブルされる、請求項 2 に記載の情報記録媒体。
- 5 1 2. 前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記情報記録媒体の用途を識別する情報が該セクタヘッダ領域に記録されている、請求項 2 に記載の情報記録媒体。
- 10 1 3. 情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード装置に送信することを認証する認証回路と
- 15 を備えた情報再生装置。
- 1 4. 前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第 1 の鍵情報と、該データ記録領域に記録される第 2 の鍵情報とを含む、請求項 1 3 に記載の情報再生装置。
- 20 1 5. 情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置から、該スクランブルされたデータを受信する前に、該鍵情報に対応する情報を該読み出し装置から受信することを認証する認証回路と、
- 25 該読み出し装置から受信した該スクランブルされたデータをデスクランブルす

るデスクランブル回路と
を備えた情報再生装置。

5 16. 前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、
前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領
域に記録される第2の鍵情報とを含む、請求項15に記載の情報再生装置。

10 17. 前記デスクランブル回路は、該第1の鍵情報に基づいて該第2の鍵情報
を変換することによって得られる情報に基づいて前記スクランブルされたデータを
デスクランブルする、請求項16に記載の情報再生装置。

15 18. 情報記録媒体から、スクランブルされたデータと該スクランブルされたデ
ータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、
該スクランブルされたデータをデスクランブルするデスクランブル回路を含む
デコード部と、
該デコード部に該スクランブルされたデータを送信する前に、該鍵情報に対応
する情報を該デコード部に送信することを認証する認証回路と
を備えた情報再生装置。

20 19. 前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、
前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領
域に記録される第2の鍵情報とを含む、請求項18に記載の情報再生装置。

25 20. 前記デスクランブル回路は、該第1の鍵情報に基づいて該第2の鍵情報
を変換することによって得られる情報に基づいて前記スクランブルされたデータを
デスクランブルする、請求項19に記載の情報再生装置。

2 1. 前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録されており、
前記情報再生装置は、

- 5 該スクランブルフラグに応じて、前記認証回路を起動するか否かを制御する制御回路をさらに備えている、請求項 1 8 に記載の情報再生装置。

2 2. 前記認証回路による認証は、所定の関数を用いて行われる、請求項 1 8 に記載の情報再生装置。

10

2 3. 前記認証回路による認証は、時間と共に変化する情報を用いて行われる、請求項 1 3、1 5 および 1 8 のいずれかに記載の情報再生装置。

15

2 4. 前記認証回路は、認証処理が正常に終了した場合にバス鍵情報を生成し、
該バス鍵情報を用いて前記第 1 の鍵情報と前記第 2 の鍵情報とを暗号化する、請求項 1 9 に記載の情報再生装置。

20

2 5. 前記認証回路は、前記バス鍵情報を用いて前記暗号化された第 1 の鍵情報と前記暗号化された第 2 の鍵情報とを復号化する、請求項 2 4 に記載の情報再生装置。

25

2 6. 情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置と、
該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置とを用いて、該スクランブルされたデータを再生する情報再生方法であって、

該読み出し装置と該デコード装置との間で相互認証処理を行うステップと、
該読み出し装置と該デコード装置との間で相互認証処理が正常に終了した場合に、該読み出し装置と該デコード装置とに共通するバス鍵情報を生成するステップと、

- 5 該バス鍵情報に応じて該鍵情報を暗号化するステップと、
 該暗号化された鍵情報を該読み出し装置から該デコード装置に送信するステップと
 を包含する情報再生方法。

図 1

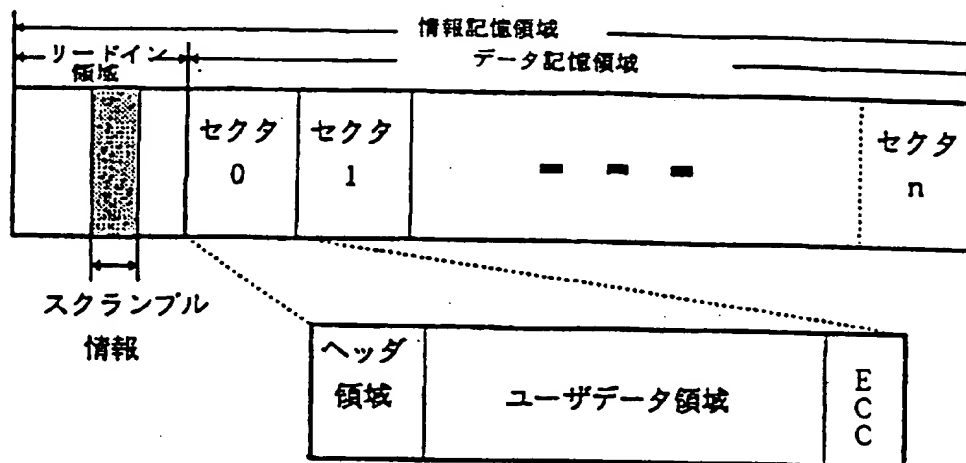


図 2

スクランブル情報	選択する初期値テーブル
0 0	テーブル 0
0 1	テーブル 1
1 0	テーブル 2
1 1	テーブル 3

(a)

テーブル 0		テーブル 1		テーブル 2		テーブル 3	
ビット列	初期値	ビット列	初期値	ビット列	初期値	ビット列	初期値
0 0 0	0000 h	0 0 0	0000 h	0 0 0	0000 h	0 0 0	000F h
0 0 1	0100 h	0 0 1	0010 h	0 0 1	0001 h	0 0 1	00F0 h
...
1 1 1	0700 h	1 1 1	0070 h	1 1 1	0007 h	1 1 1	0FFF h

(b)

図 3

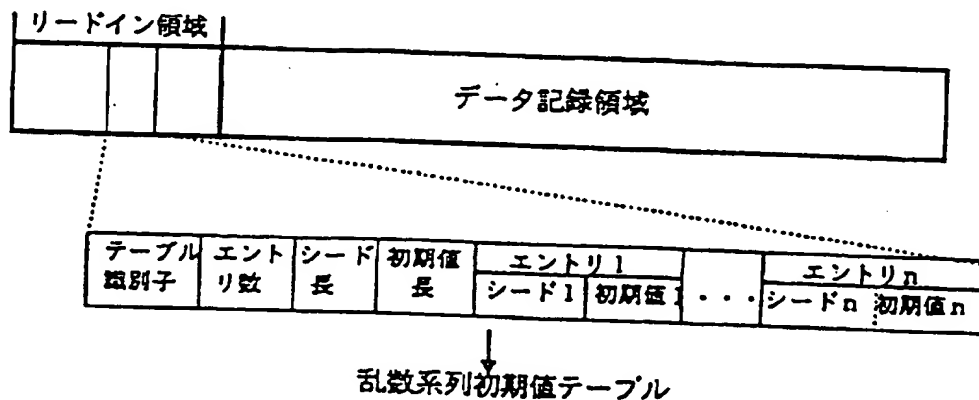


図 4

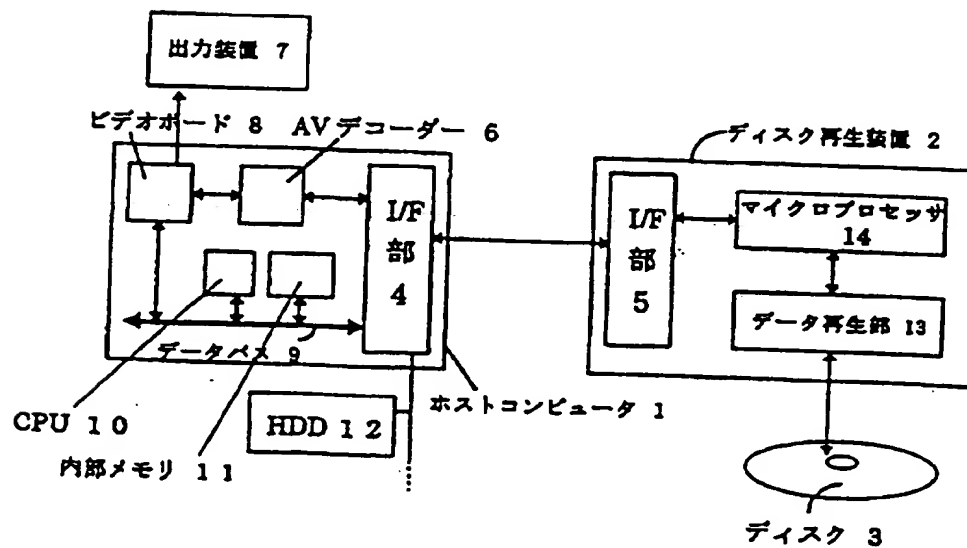


図 5

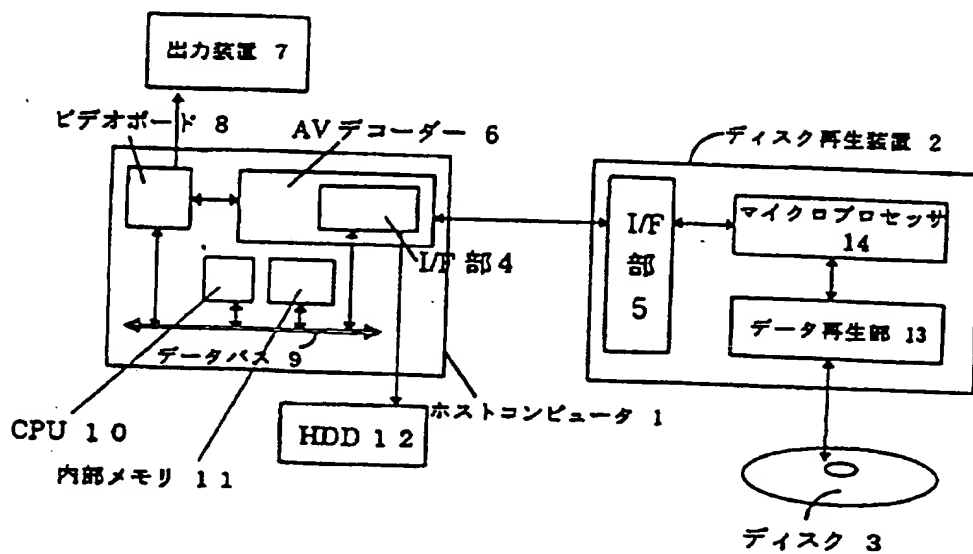


図 6

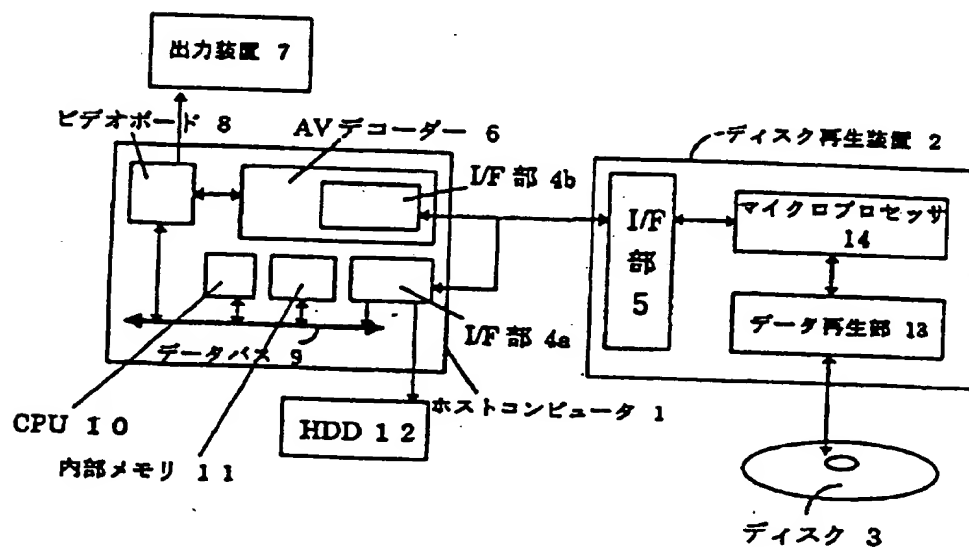


図 7

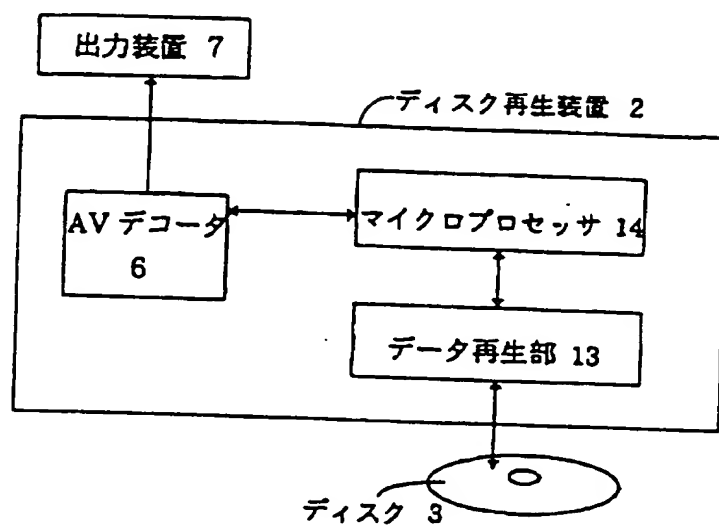


図 8

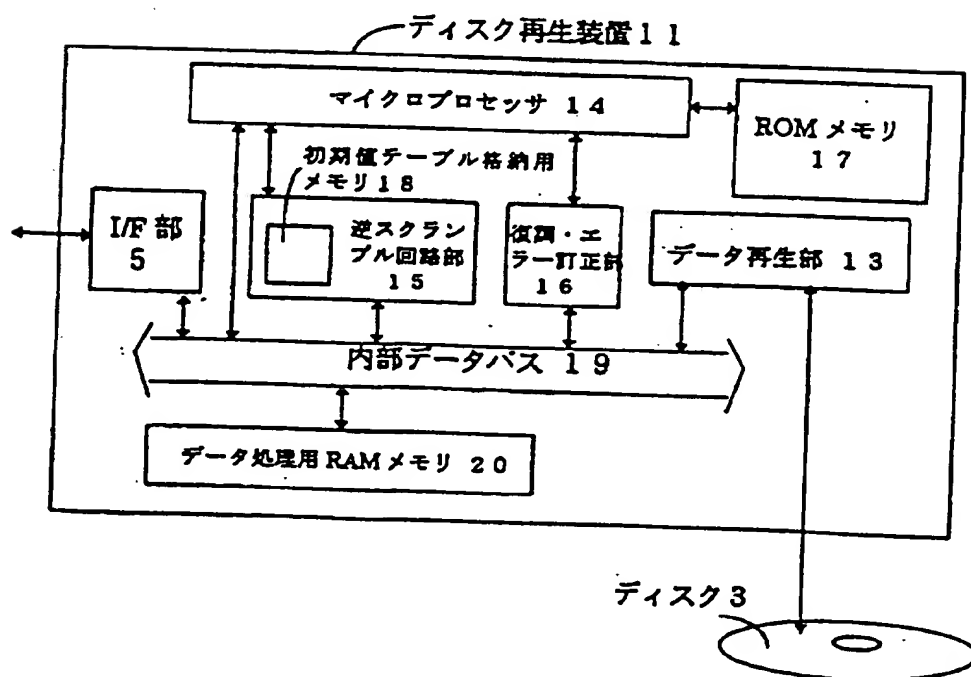
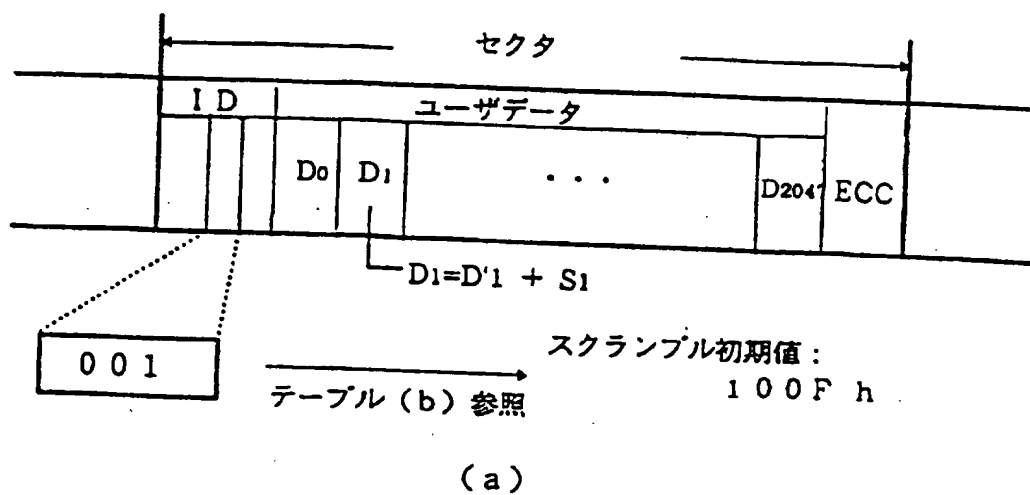


図 9



ビット列	スクランブル初期値	乱数系列			
		S0	S1	...	S2047
000	0000h	A0	A1	...	A2047
001	100Fh	B0	B1	...	B2047
...			
111	5FFFh	C0	C1	...	C2047

(b)

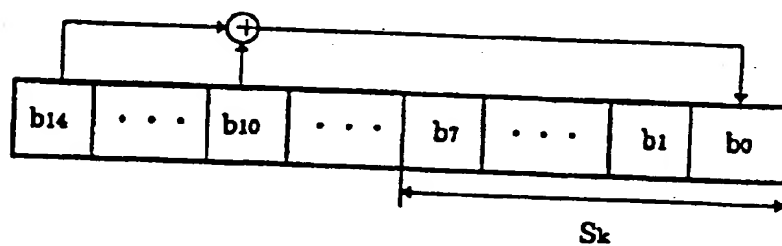


図 10

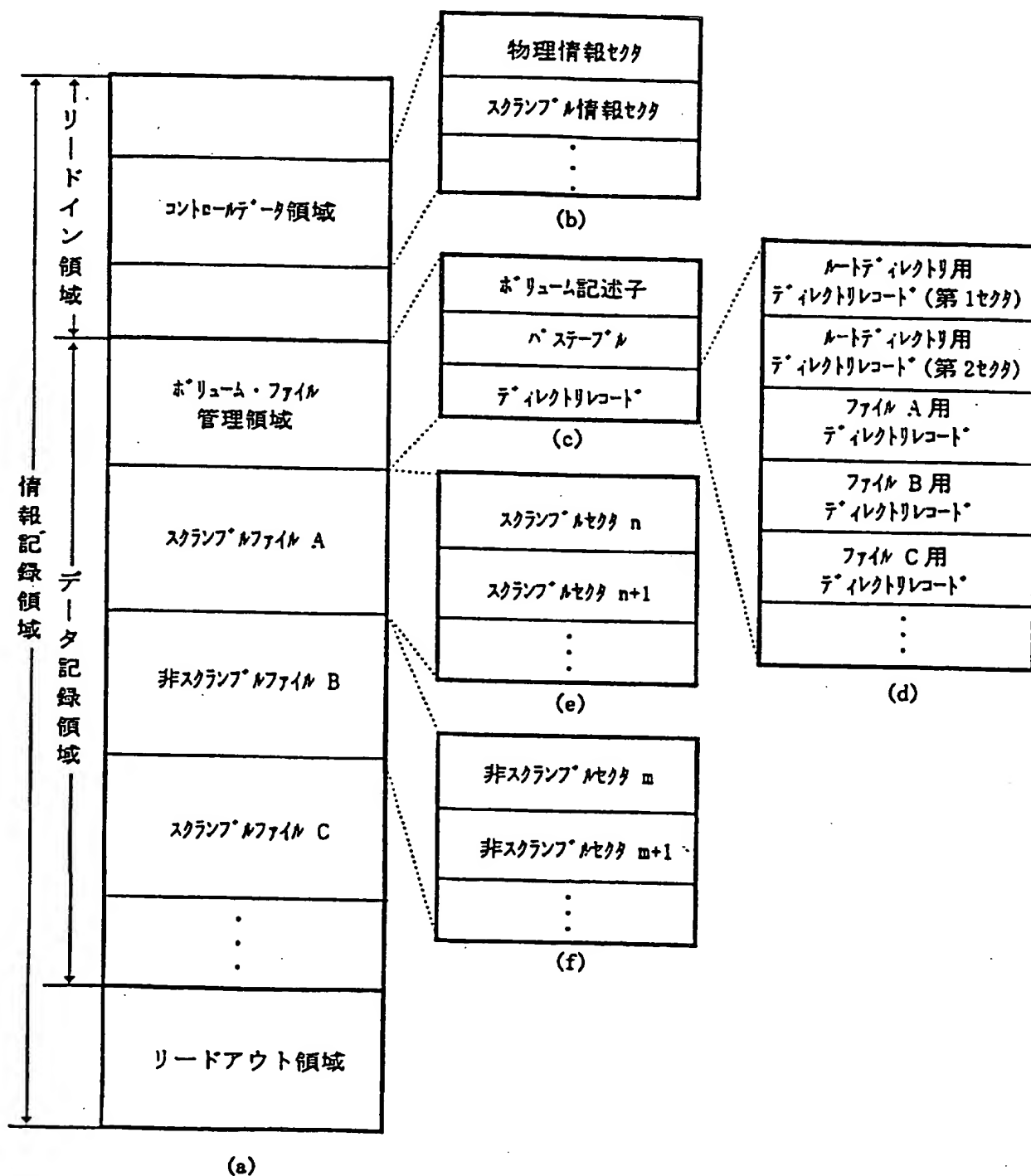


図 11

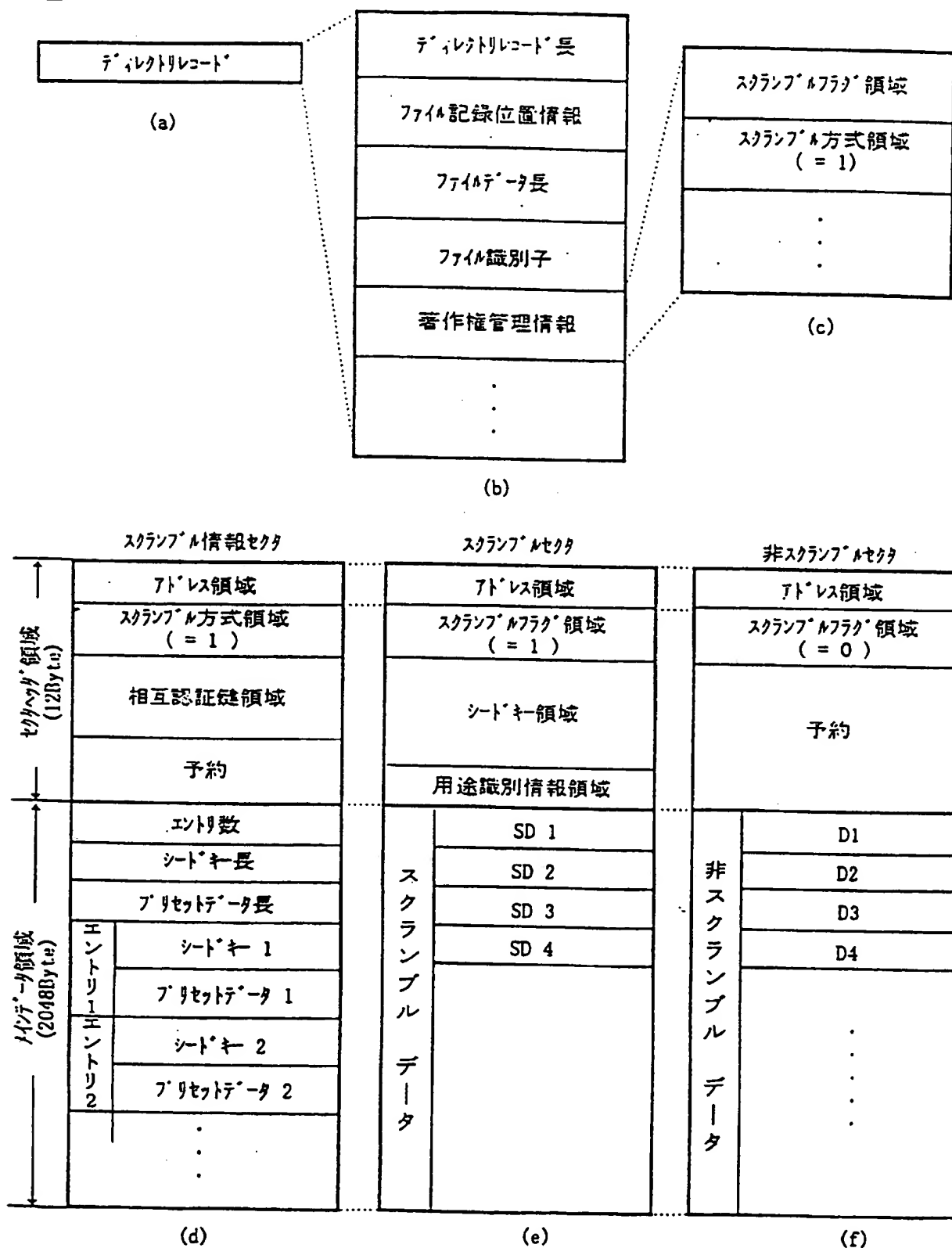


図 12

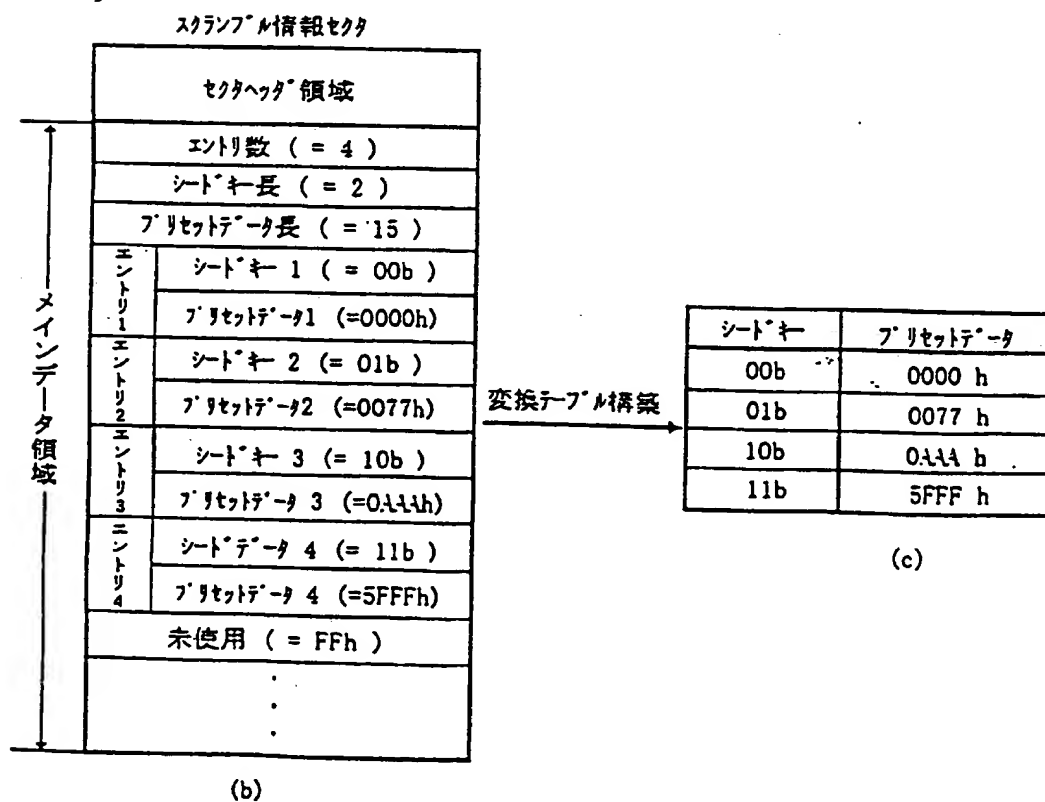
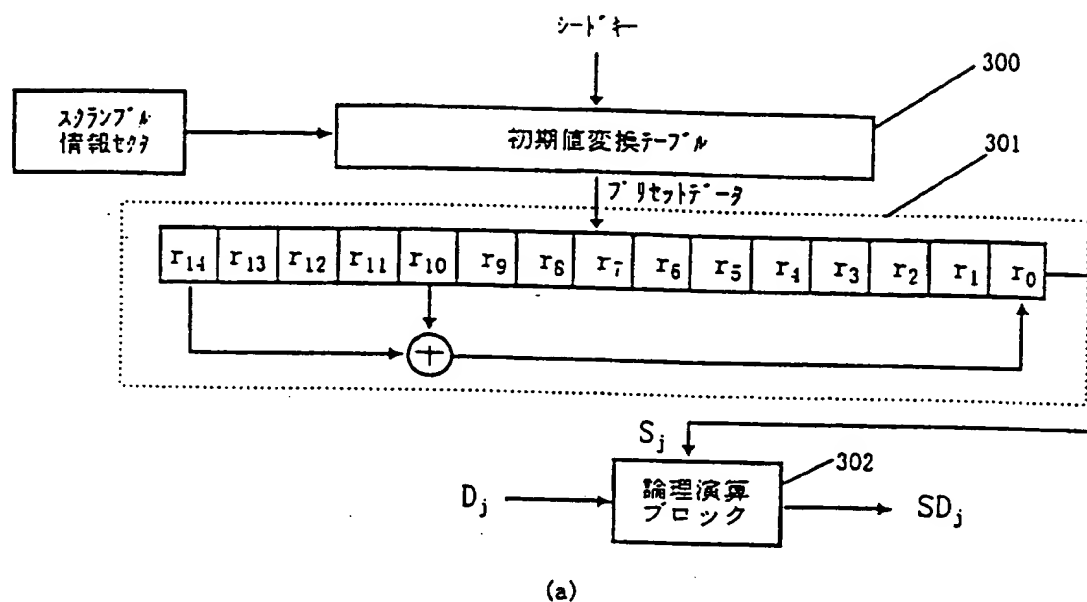


図 1 3

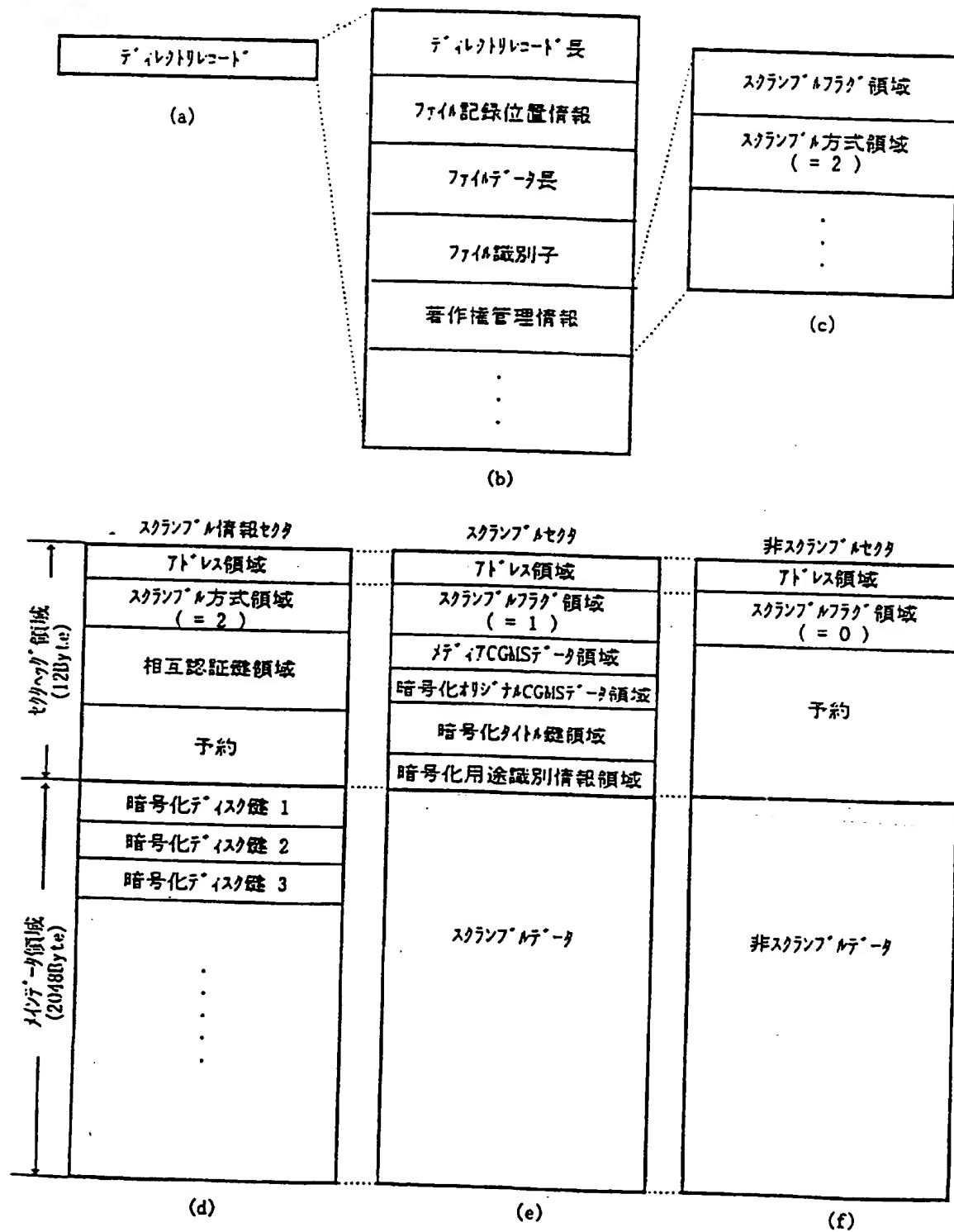


図 14

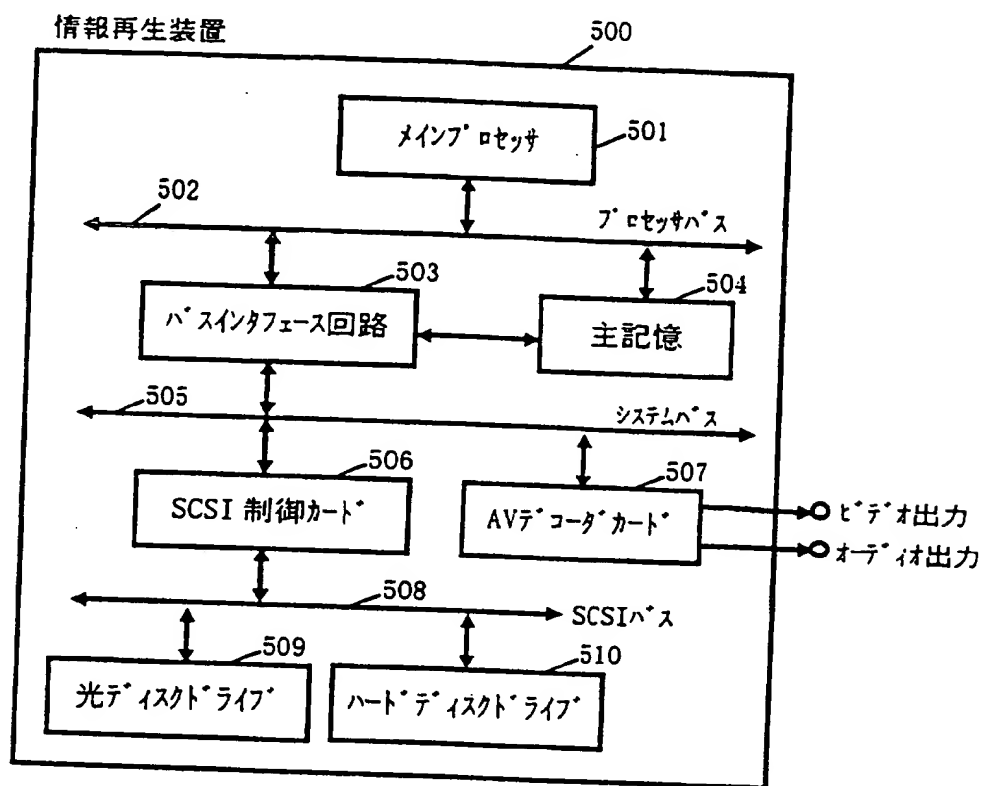


図 15

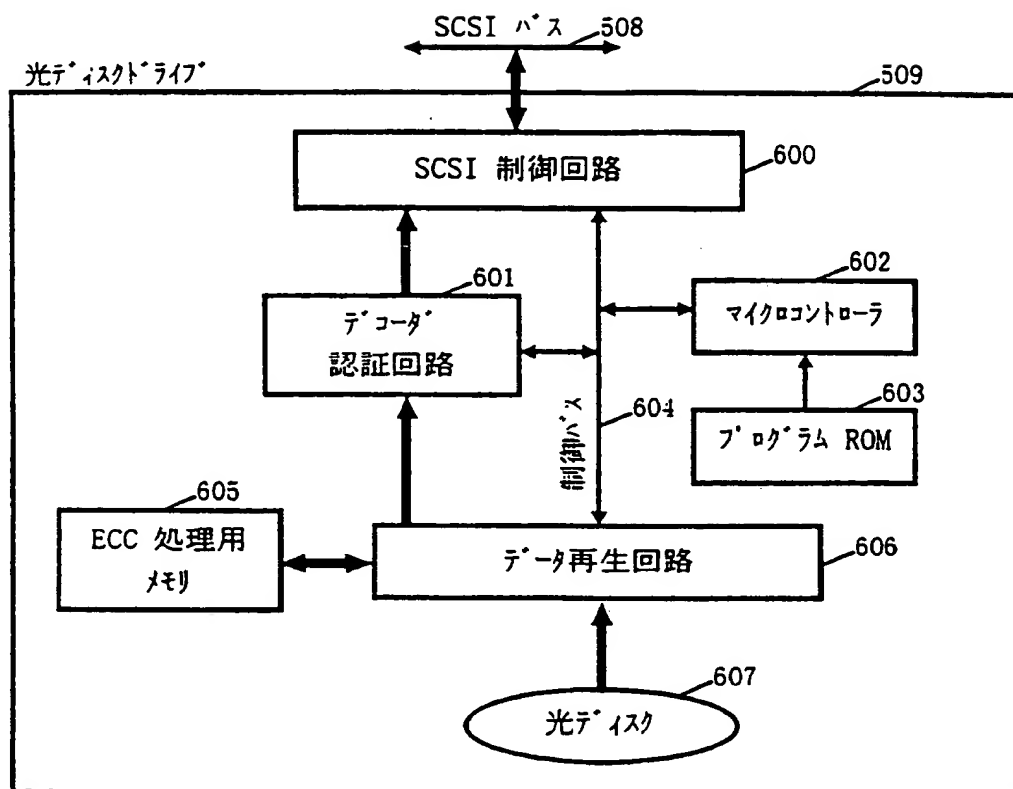


図 16

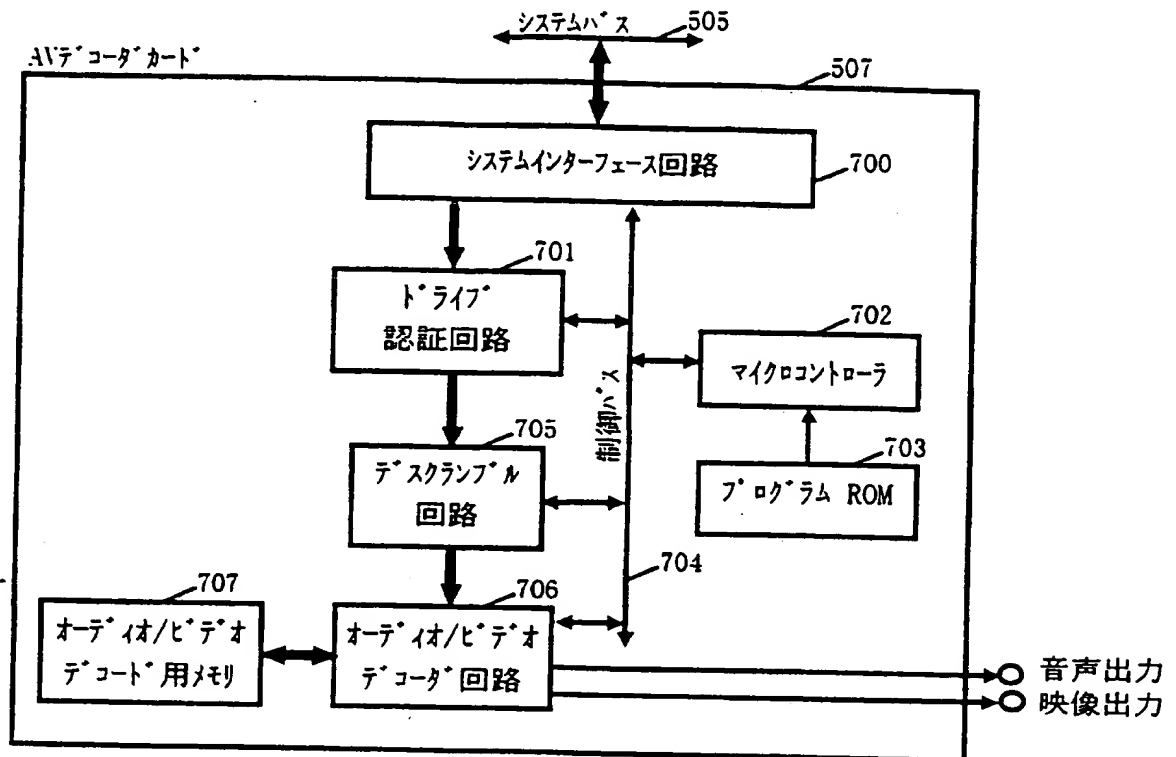


図 17

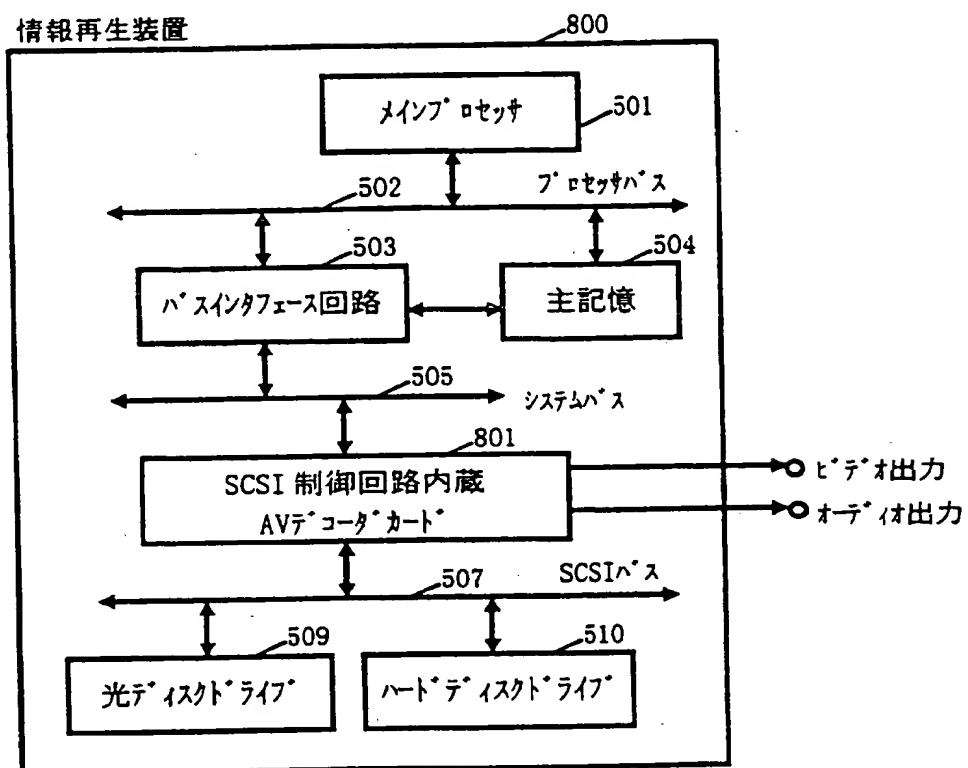


図 18

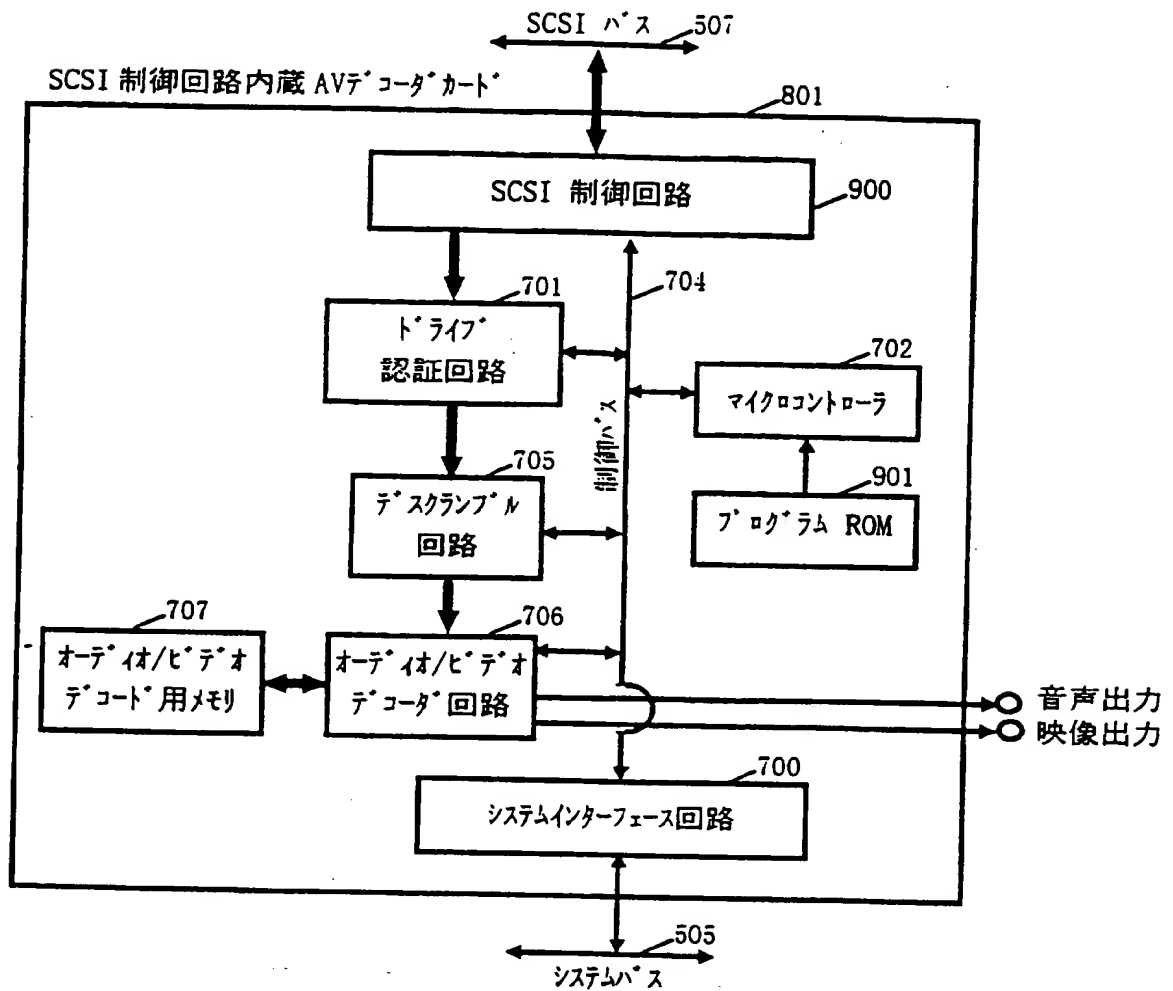


図 19

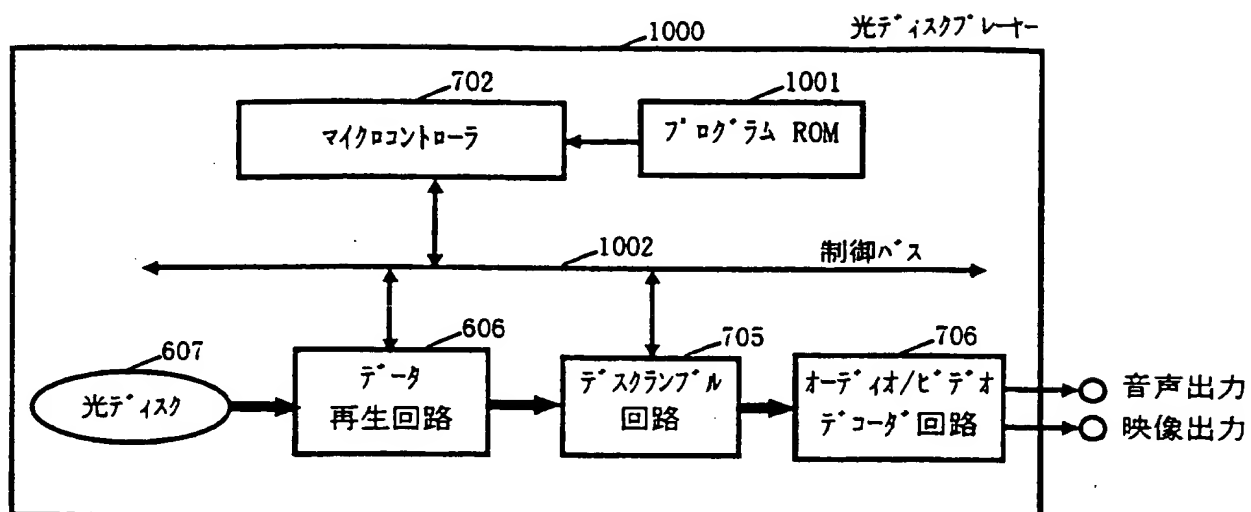


図 20

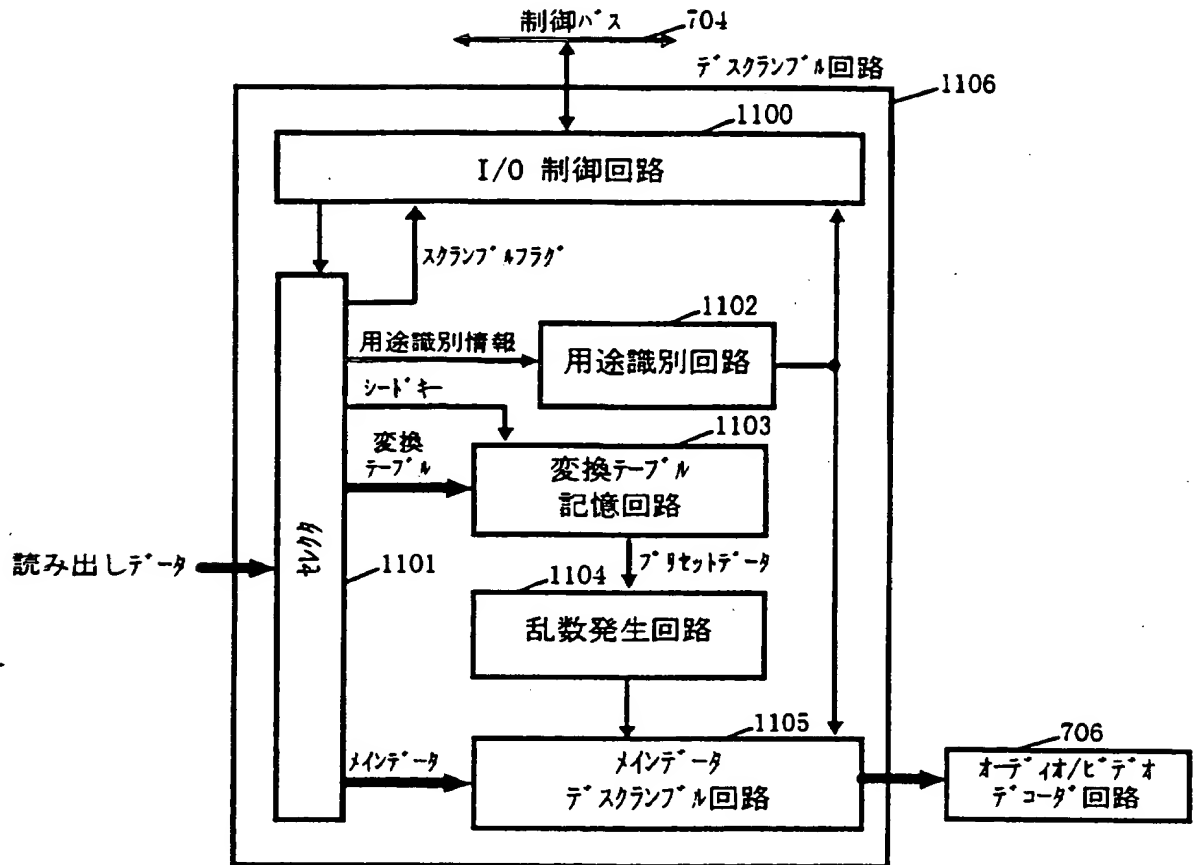


図 21

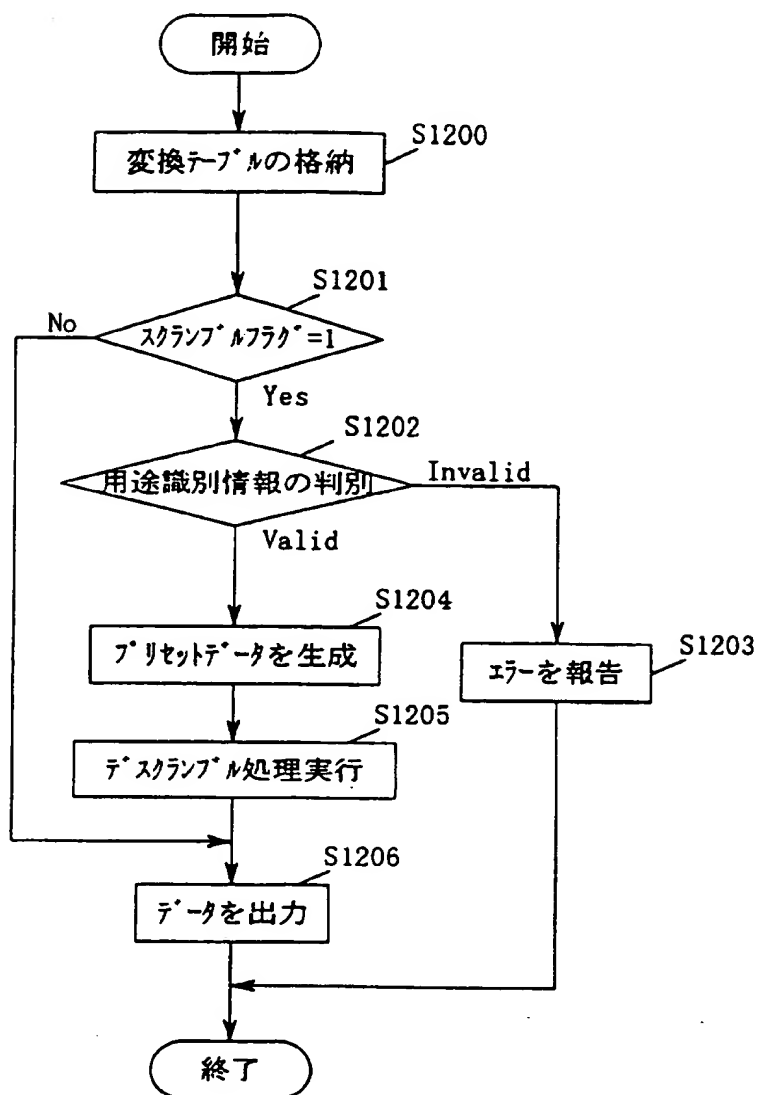


図 22

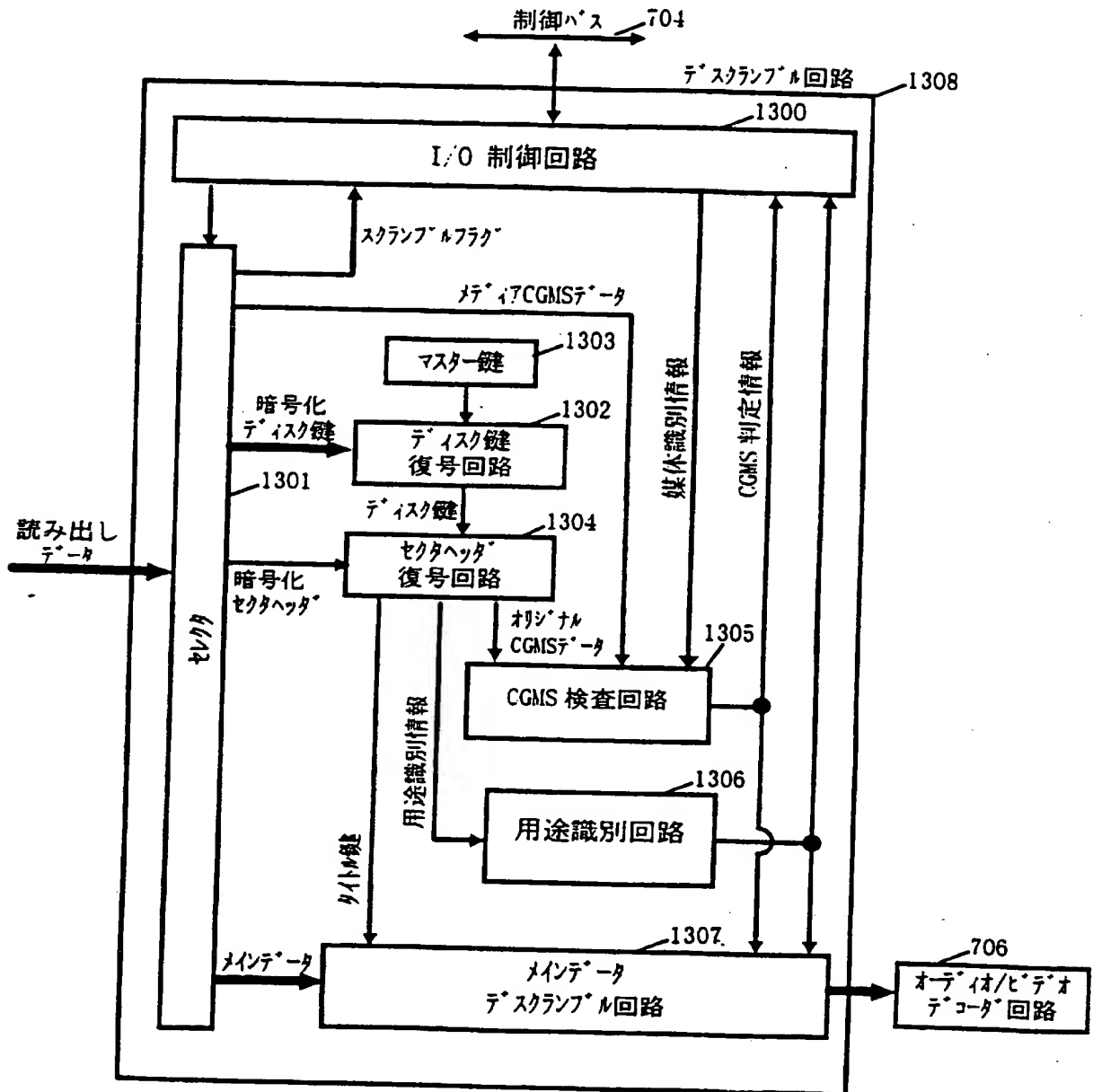


図 23

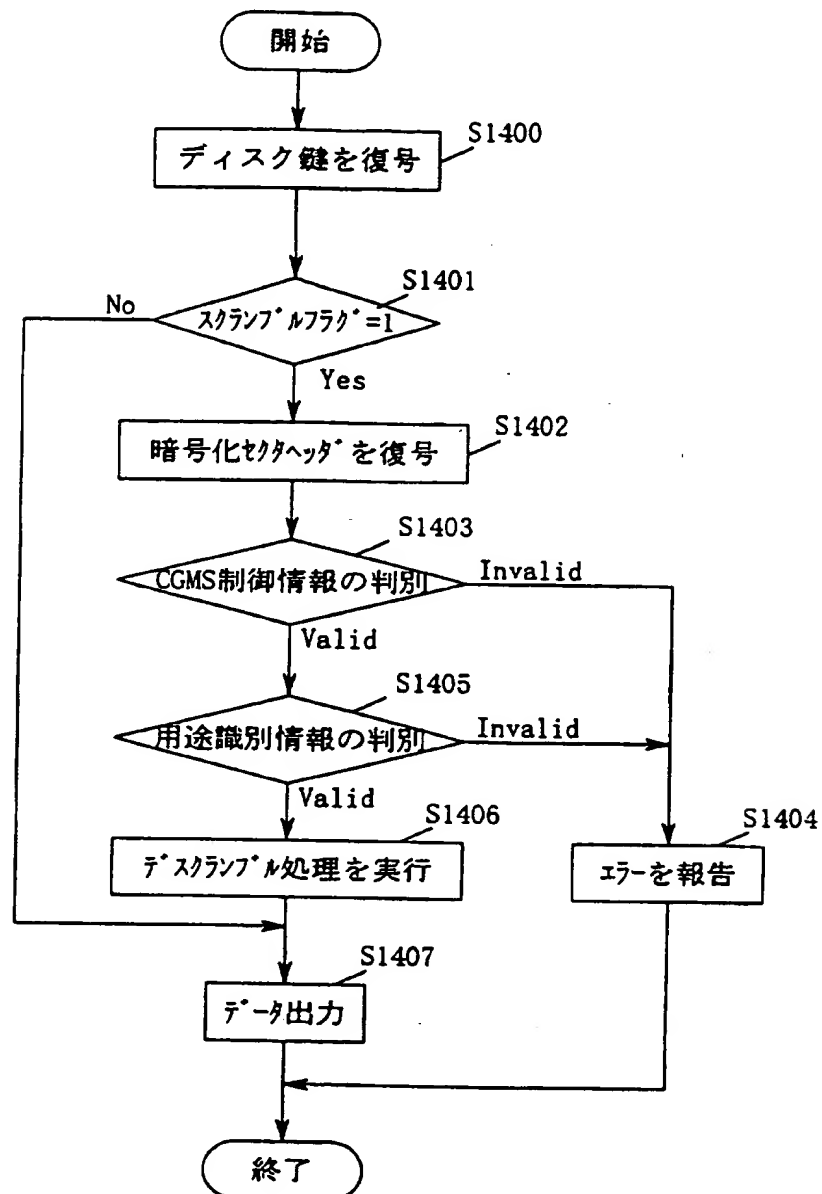


図 2 4

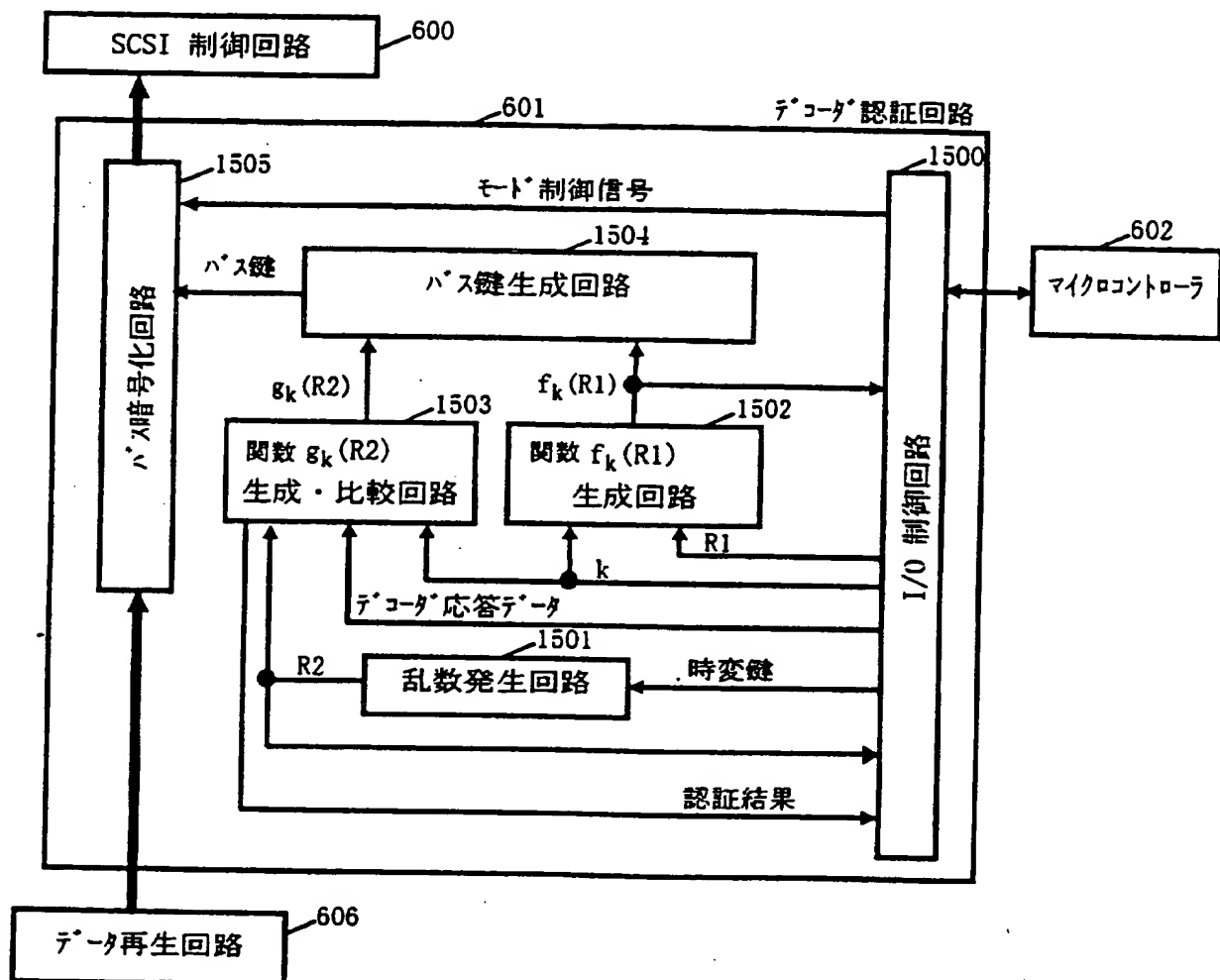


図 25

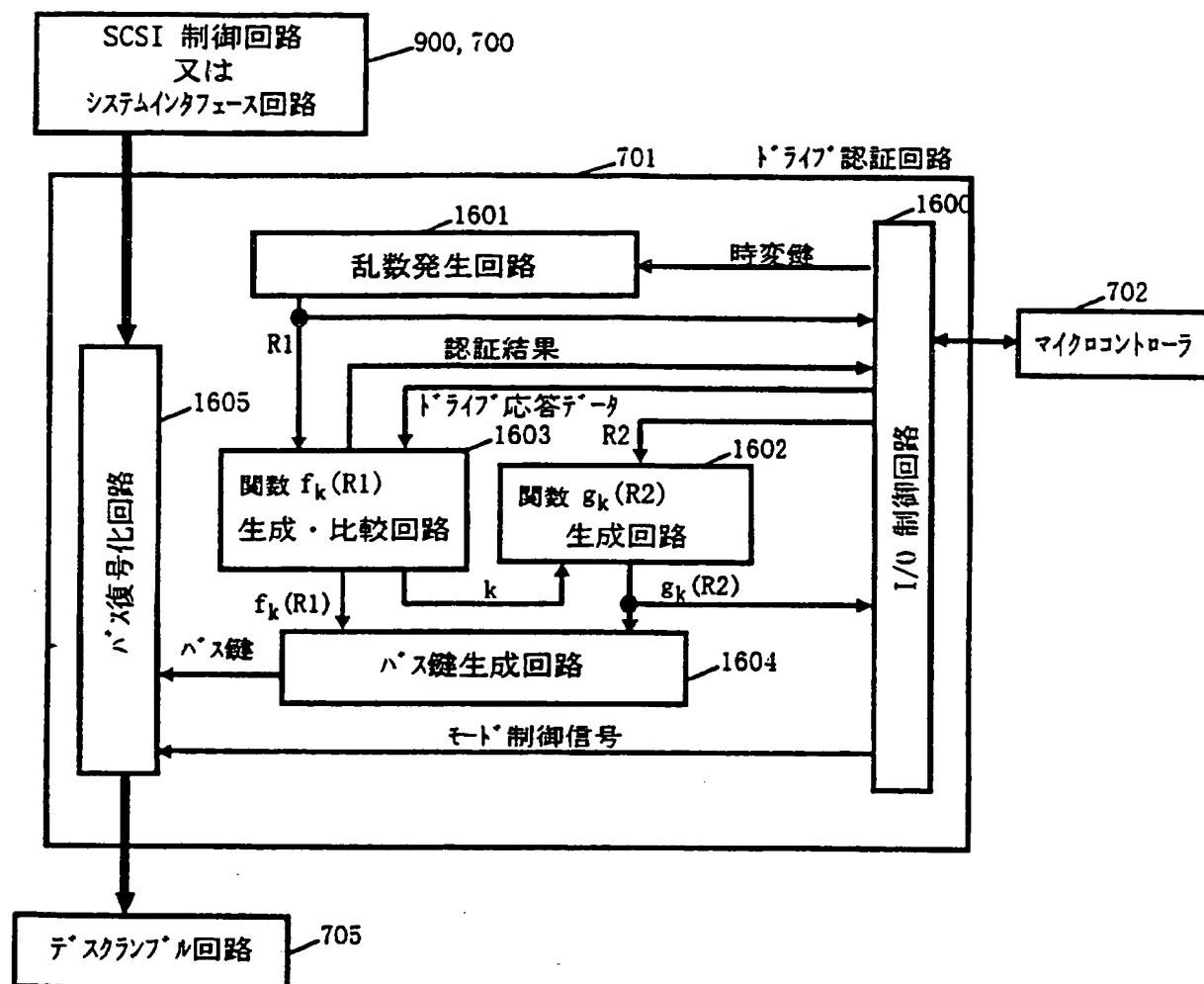
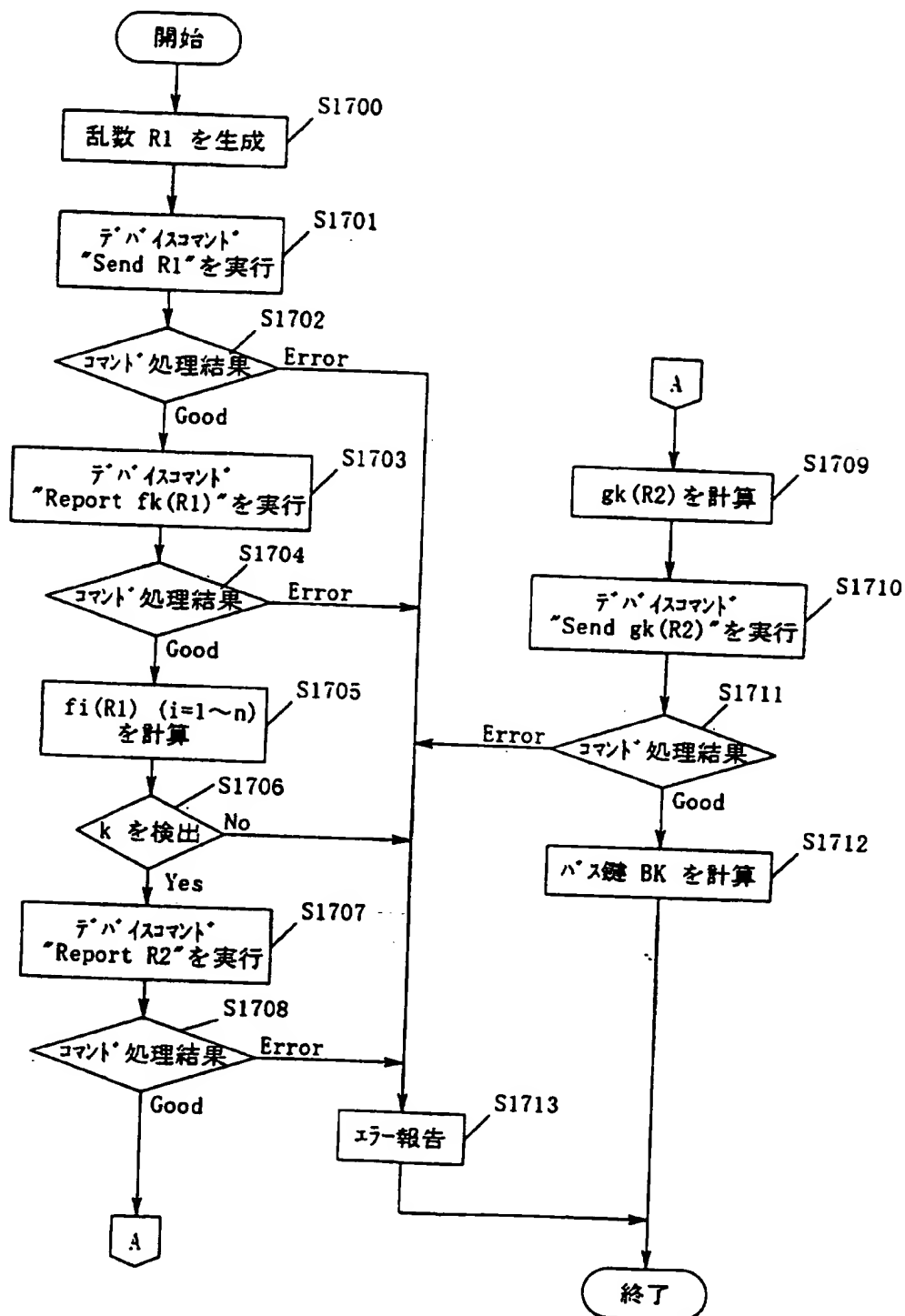


図 26



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP96/02901

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl⁶ G11B19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl⁶ G11B19/00, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926 - 1996
Kokai Jitsuyo Shinan Koho	1971 - 1996
Toroku Jitsuyo Shinan Koho	1994 - 1996

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 62-89275, A (Sanyo Electric Co., Ltd.), April 23, 1987 (23. 04. 87) (Family: none)	1
A	JP, 7-85574, A (Victor Co. of Japan, Ltd.), March 31, 1995 (31. 03. 95) (Family: none)	1 - 26
A -	JP, 7-21688, A (Victor Co. of Japan, Ltd.), January 24, 1995 (24. 01. 95) (Family: none)	1 - 26
A	JP, 7-249264, A (Intec Inc., Brother Industries Ltd.), September 26, 1995 (26. 09. 95) (Family: none)	1 - 26
Y	JP, 4-256196, A (Toshiba Corp.), September 10, 1992 (10. 09. 92) (Family: none)	2 - 4
A	JP, 6-133314, A (Matsushita Electric Industrial Co., Ltd.), May 13, 1994 (13. 05. 94) (Family: none)	1 - 26
A	JP, 6-169307, A (Sony Corp.),	1 - 26

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

 Date of the actual completion of the international search
 January 28, 1997 (28. 01. 97)

 Date of mailing of the international search report
 February 12, 1997 (12. 02. 97)

 Name and mailing address of the ISA/
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP96/02901

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P	<p>June 14, 1994 (14. 06. 94) (Family: none)</p> <p>JP, 7-288798, A (Mitsubishi Electric Corp.), October 31, 1995 (31. 10. 95) (Family: none)</p>	1 - 26

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁸ G11B19/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁸ G11B19/00, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国 実用新案公報 1926-1996
 日本国 公開実用新案公報 1971-1996
 日本国 登録実用新案公報 1994-1996

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 62-89275, A (三洋電機株式会社) 23. 4月. 1987 (23. 04. 87) (ファミリーなし)	1
A	J P, 7-85574, A (日本ビクター株式会社) 31. 3月. 1995 (31. 03. 95) (ファミリーなし)	1-26
A	J P, 7-21688, A (日本ビクター株式会社) 24. 1月. 1995 (24. 01. 95) (ファミリーなし)	1-26
A	J P, 7-249264, A (株式会社インテック, プラザー工業株式会社) 26. 9月. 1995 (26. 09. 95) (ファミリーなし)	1-26

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 先行文献ではあるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

28. 01. 97

国際調査報告の発送日

12.02.97

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100

東京都千代田区蔵が関三丁目4番3号

特許庁審査官 (権限のある職員)

菅澤 洋二

印

5D

7618

電話番号 03-3581-1101 内線 6921

C (続き) . 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 4-256196, A (株式会社東芝) 10. 9月. 1992 (10. 09. 92) (ファミリーなし)	2-4
A	JP, 6-133314, A (松下電器産業株式会社) 13. 5月. 1994 (13. 05. 94) (ファミリーなし)	1-26
A	JP, 6-169307, A (ソニー株式会社) 14. 6月. 1994 (14. 06. 94) (ファミリーなし)	1-26
P	JP, 7-288798, A (三菱電機株式会社) 31. 10月. 1995 (31. 10. 95) (ファミリーなし)	1-26